Juniper tietoturvaominaisuudet SpiderNet-ympäristössä

Vesa-Ville Kaipainen

Opinnäytetyö
Toukokuu 2011

Tietoverkkotekniikka
Tekniikka ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t) KAIPAINEN, Vesa-Ville	Julkaisun laji Opinnäytetyö	Päivämäärä 18.05.2011
	Sivumäärä 92 + 56	Julkaisun kieli Suomi
	Luottamuksellisuus ( ) saakka	Verkkojulkaisulupa myönnetty (X)
Työn nimi Juniper tietoturvaominaisuudet Spidernet-ympäristössä		
Koulutusohjelma Tietoverkkotekniikka		
Työn ohjaaja(t) LEINO, JANNE		
Toimeksiantaja(t) Jyväskylän ammattikorkeakoulu Oy VATANEN, MARKO		

Tiivistelmä

SpiderNet on Jyväskylän ammattikorkeakoulun Teknologia-yksikön laboratorioympäristö. SpiderNet-laboratoriota käytetään pääsääntöisesti tietoverkkotekniikan koulutusohjelman opintojaksoilla, mutta sitä käytetään laajasti myös tutkimus- ja kehitystöissä, kuten opinnäytetöissä. SpiderNet on täysin erotettuna Jyväskylän ammattikorkeakoulun tuotantoverkosta.

Opinnäytetyön tarkoituksena oli tutkia ja implementoida Juniper Networks J-series reitittimien tietoturvaominaisuuksia SpiderNet-laboratorioympäristössä. Työn teko aloitettiin tutustumalla Junos-käyttöjärjestelmään, joka on käytössä kaikissa Juniper Networksin laitteissa riippumatta käyttötarkoituksesta.

Työssä rakennettiin SpiderNet-laboratorioympäristön laitteista kokonaisuus, jossa pystyttiin simuloimaan ”Internetiä”, sekä yrityksen kolmea eri paikassa sijaitsevaa toimipistettä. Tämä topologia mahdollisti tietoturvaominaisuuksien monipuolisen konfiguroinnin ja niiden toimivuuden todentamisen. Työssä oli neljä suurempaa kokonaisuutta: turva-alueet ja -säännöt, Screenit, Network Address Translation (NAT) sekä IPSec VPN-yhteydet.

Työn tuloksena saatiin testattua ja todennettua haluttujen tietoturvaominaisuuksien toiminta. Lisäksi tehtiin kaksi tietoturva-aiheista laboratorioharjoitusta, jotka on tarkoitus sisällyttää tuleville tietoturvakursseille.

Avainsanat (asiasanat)
IDP, IPSec, JUNOS, SpiderNet, Tietoturva, VPN

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s)	Type of publication	Date
KAIPAINEN, Vesa-Ville	Bachelor´s Thesis	18.05.2011
	Pages 92 + 56	Language Finnish
	Confidential ( ) Until	Permission for web publication (x)

TITLE
JUNIPER SECURITY IN SPIDERNET

Degree Programme
Data Network Technology

Tutor(s)
LEINO, Janne

Assigned by
JAMK University of Applied Sciences
VATANEN, Marko

Abstract

SpiderNet is a laboratory at JAMK University of Applied Sciences. SpiderNet is mainly used for data network technology courses and also used on various research and development projects such as Bachelor's Theses. SpiderNet is completely separated from Jyväskylä University of Applied Sciences' production Network.

The main goal of this thesis was to study and implement the main security characteristics of Juniper Networks J-series routers at SpiderNet-laboratory. The project began with studying the Junos Operating System, which is used at every Juniper Networks device regardless of the purpose of the device.

The thesis consisted of building a network topology from SpiderNet laboratory's equipment that simulated the Internet and a corporate network with three offices. This topology provides an environment where testing and configuring security configuration is possible. The thesis focused on four major parts: Security Zones and Policies, Screens, Network Address Translation (NAT) and IPSec VPN.

The result of this thesis were successfully configured and tested security characteristics and two laboratory exercises which are going to be a part of future data security education at JAMK.

Keywords
IDP, IPSec, JUNOS, SpiderNet, Security, VPN

Miscellaneous

SISÄLTÖ

KUVIOT

TAULUKOT

LYHENTEET

AES	Advanced Encryption Standard
AH	Authentication Header
ALG	Application Layer Gateway
ARP	Address Resolution Protocol
CoS	Class of Service
DES	Data Encryption Standard
DH	Diffie-Hellman
DNS	Domain Name Server
DoS	Denial of Service
ESP	Encapsulating Security Payload
HMAC	Hash-based Message Authentication Code
ICMP	Internet Control Message Protocol
IDP	Intrusion Detection and Prevention
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
MD5	Message-Digest Algorithm
NAT	Network Address Translation
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PFS	Perfect Forward Secrecy
SA	Security Association
SHA	Secure Hash Algorithm
SSH	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

1 TYÖN KUVAUS

1.1 Toimeksiantaja

Opinnäytetyön toimeksiantajana toimi Jyväskylän ammattikorkeakoulun (Jamk) tietotekniikan koulutusala. Jyväskylän ammattikorkeakoululla on toimipisteitä Jyväskylässä sekä Saarijärven Tarvaalassa. Jyväskylän ammattikorkeakoulu tarjoaa korkeakoulututkintoon johtavaa koulutusta, ammatillista opettajakoulutusta, avoimia ammattikorkeakouluopintoja, täydennyskoulutusta ja myös oppimistyyppistä täydennyskoulutusta nuorille ja aikuisille. Oppilaita Jyväskylän ammattikorkeakoulussa on jo yli 8000. (Jyväskylän ammattikorkeakoulu 2011a.)

Jyväskylän ammattikorkeakoululla on vahva asema Jyväskylän seudun ja Keski-Suomen kehittäjien joukossa. JAMK:lla on kiinteät suhteet alueen yrityksiin ja yhteisöihin, mikä näkyy valmistuneiden työllistymisprosenteistakin. Valmistuneista 74 prosenttia on töissä vuoden kuluttua valmistumisesta. (Jyväskylän ammattikorkeakoulu 2011a.)

Tietotekniikan koulutusohjelmassa paneudutaan suurimmaksi osaksi tietoverkkotekniikan osa-alueelle. Painopisteinä ovat mm. laajakaista, langattomat ja langalliset operaattoritason teknologiat, verkkojen ylläpito ja suunnittelu sekä tietoturvallisuuden hallinta. Opintojen konkreettisuuden mahdollistaa Jyväskylän ammattikorkeakoulun oma SpiderNet laboratorioympäristö, johon pääsee tutustumaan läheisesti opintojen aikana. (Jyväskylän ammattikorkeakoulu 2011b.)

1.2 Tavoitteet

Työn tavoitteena oli tutkia Juniper Networksin J-2320 reitittimien tietoturvaominaisuuksia ja tehdä niistä myös käytännön harjoitteita. J-2320 reitittimet ovat osa SpiderNet laboratorioympäristöä, jossa työ toteutettiin. Työssä käytettiin Cisco Systemsin ja Juniper Networksin laitteita.

Tavoitteena oli muodostaa SpiderNetin laitteista yrityksen pääkonttoria ja kahta sivukonttoria simuloiva verkko. Pääkonttorin olisi tarkoitus sisältää yhden Juniper Networks J-series -reitittimen sekä kaksi Ciscon kytkintä. Kahden sivukonttorin laitekoonpanoissa ei ollut muuta eroa, kuin toisessa Juniper Networksin J2320-reititin kor-

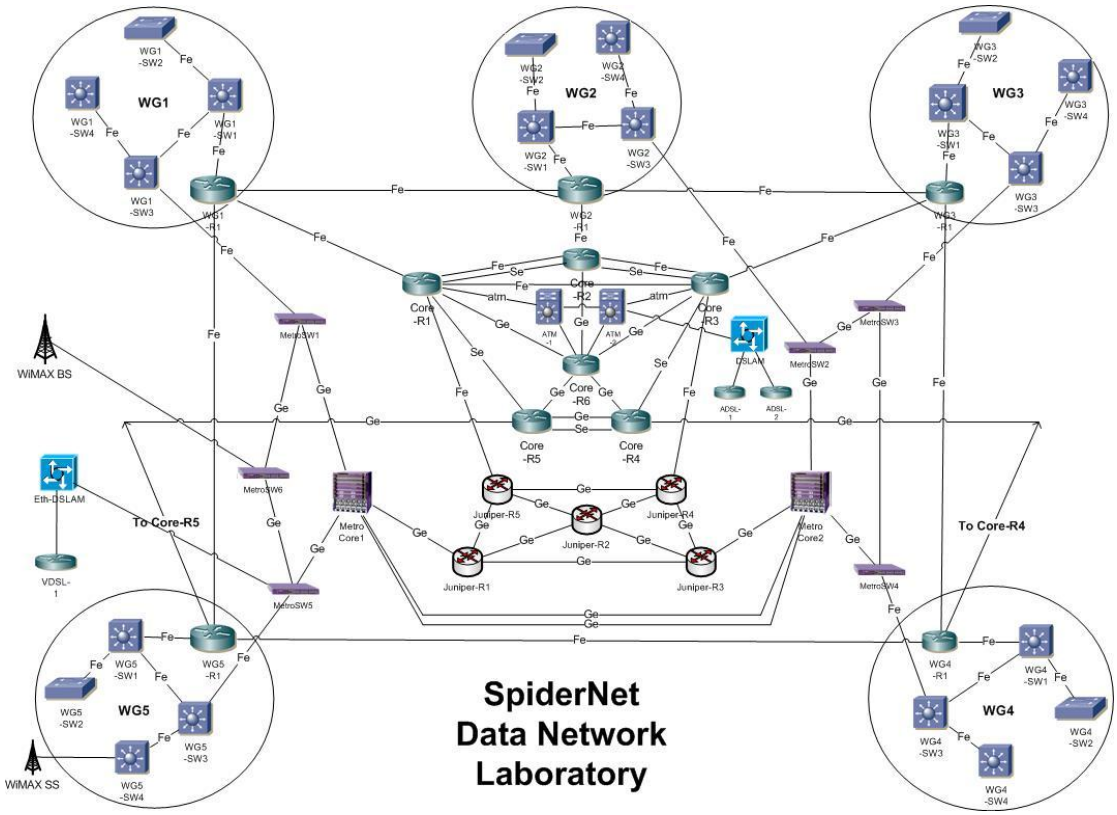
vattiin Ciscon reitittimellä. Käyttämällä myös Ciscon reititintä yhdessä sivukonttorissa, oli mahdollista testata VPN-yhteys Cisco Systemsin ja Juniper Networksin välillä. Pääkonttorin ja sivukonttoreiden reitittimet oli tarkoitus liittää kolmeen erilliseen Cisco Systemsin reitittimeen, jotka simuloisivat Internetiä.

Tietoturvaominaisuuksien testauksen lisäksi oli tavoitteena tehdä kaksi laboratoriohar-joitusta. Ensimmäisessä käytäisiin läpi turvasäännöt (security policy), Screenit sekä Network Address Translation (NAT). Toisessa harjoitteessa muodostettaisiin Virtual Private Network (VPN) yhteys Internetin läpi kahden työryhmän välille.

2 SpiderNet

2.1 Yleistä

Jyväskylän ammattikorkeakoulun teknologiayksikön tietoverkkotekniikan koulutusohjelman käytännönharjoitteiden laboratorioympäristö on nimeltään SpiderNet. SpiderNetiä on kehitetty jo yli kymmenen vuotta ja sitä kehitetään jatkuvasti uusien teknologioiden mukana. SpiderNet on täysin erotettuna Jyväskylän ammattikorkeakoulun tuotantoverkosta. SpiderNetiä käytetään pääasiassa useilla tietoverkkotekniikan koulutusohjelman opintojaksoilla, mutta sitä käytetään myös tutkimus- ja kehitystöissä. SpiderNet on myös loistava ympäristö opinnäytetöiden teolle. Koko SpiderNetin topologia selviää kuviosta 1. (Spidernet 2011.)



KUVIO 1. SpiderNet –topologia
(SpiderNet 2011)

2.2 Laitteisto ja topologia

Tällä hetkellä laboratorioympäristössä on käytössä seuraavien laitevalmistajien laitteita: Airspan Networks, Cisco Systems, Extreme Networks, Juniper Networks ja Zhones. SpiderNet laboratorioympäristö koostuu neljästä isommasta kokonaisuudesta: Cisco Core, Metro Core, Juniper Core sekä viisi työryhmää. (SpiderNet 2011.)

2.3 Keskuskytkin (Center Switch)

Vuonna 2010 SpiderNetiin lisättiin ns. keskuskytkin (centerswitch), eli kytkin, joka on yhteydessä kaikkiin SpiderNetistä löytyviin kytkimiin ja reitittimiin. Tämä helpottaa erilaisten topologioiden rakentamista ilman, että tarvitsee yhdistellä piuhoja kytkinkaapeissa, vaan topologien rakentelu hoituu keskuskytkimen kautta käyttäen eri yhteyksille eri VLAN:ia.

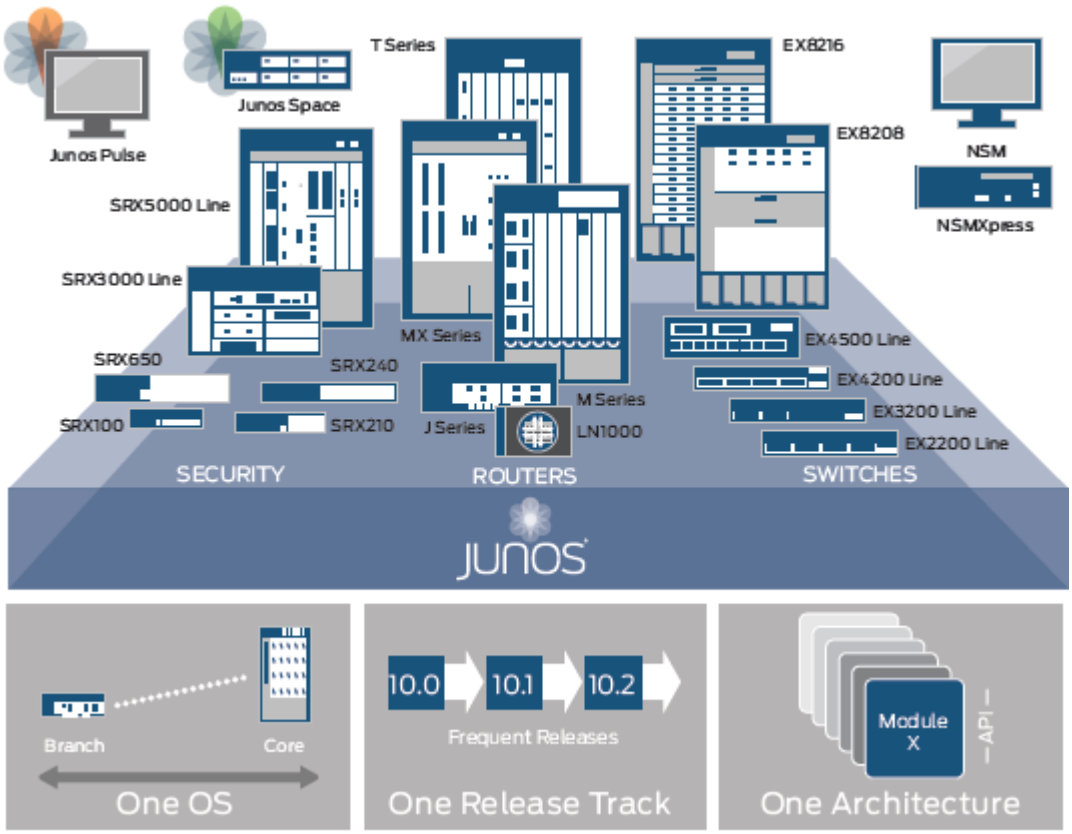
3 Juniper Networks

3.1 Taustaa Juniper Networks -yrityksestä

Juniper Networks on perustettu vuonna 1996 Kaliforniassa. Juniper Networks on yli kahdeksan tuhannen työntekijän yritys, joka on levinnyt 47 maahan ja joka tarjoaa palveluitaan n. sadalle verkko-operaattorille, yli 30000 yritykselle ja sadoille julkisen sektorin organisaatioille. Juniper Networks tarjoaa laajan valikoiman palveluita, jotka kattavat mm. reitityksen, kytkemisen, tietoturvan, identiteetin hallinnan sekä laitteistojen hallinnoinnin, joka tarjoaa ainutlaatuisen suorituskyvyn, suuren määrän valintoja sekä joustavuutta. (Juniper Networks 2011a.)

3.2 Junos-käyttöjärjestelmä

Juniper Networksin käyttöjärjestelmä Junos tarjoaa yhteisen kielen Juniper Systemsin laitteiden hallintaan, oli sitten kyse reitittimistä, kytkimistä tai tietoturvalaitteista (ks. kuvio 2). Junosin avulla uuden työntekijän koulutus on helpompaa, päivittäiset toimenpiteet hoituvat tehokkaammin ja muutosten teko onnistuu nopeammin. Koska Junos on käytössä kaikissa Juniper Networksin laitteissa, sen päivittäminen onnistuu kaikkiin laitteisiin samanaikaisesti julkaistavalla päivityksellä. Junos-käyttöjärjestelmä päivitetään neljä kertaa vuodessa. (Juniper Networks 2011b.)



KUVIO 2. Junos-käyttöjärjestelmä
(Juniper Networks 2011b)

Junos käyttöjärjestelmä on arkkitehtuuriltaan modulaarinen. Tämä mahdollistaa joustavan, vakaan sekä innovatiivisen verkon toiminnan. Modulaarisuuden hyötynä on erittäin vakaa alusta. Moduulit toimivat itsenäisesti niiden omissa suojatuissa muisteissa, joten yhden moduulin virhetoiminto ei voi kaataa toista moduulia kuormittamalla muiden moduulien muistia. Modulaarinen arkkitehtuuri pystyy myös erottamaan hallinta- ja välitystoiminnot toisistaan, mikä mahdollistaa tehokkaan suorituskyvyn niin pieniin, kuin suuriinkin laitteisiin. (Juniper Networks 2011a.)

4 Tietoturva Juniper Networks J-series reitittimissä

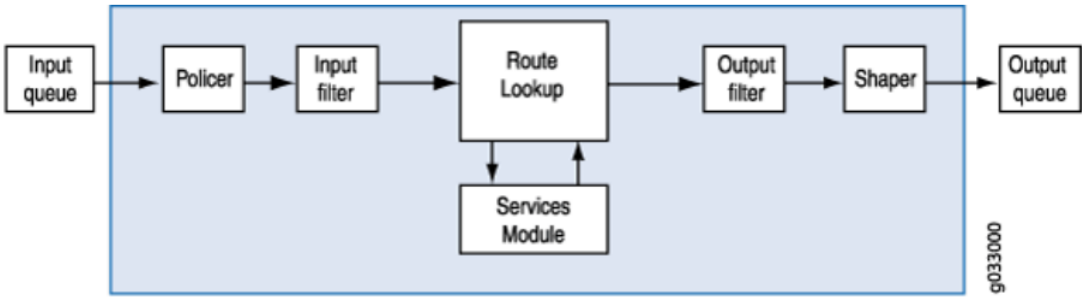
4.1 Tiedonsiirto

4.1.1 Yleistä

Paketit, jotka liikkuvat J-series-reitittimen sisälle tai ulos, käyvät läpi joko pakettipohjaisen (packet-based) prosessin tai vuopohjaisen (flow-based) prosessin. Pakettipohjainen eli tilaton prosessointi käy liikenteen läpi paketti kerrallaan. Vuopohjainen eli tilallinen menettelytapa käsittelee liikennettä istunnoissa. (Juniper Networks Security Configuration Guide 2011, 93.)

4.1.2 Pakettipohjainen prosessointi

Pakettipohjainen prosessointi tapahtuu yksi paketti kerrallaan huolimatta siitä, ovatko tulevat paketit mahdollisesti menossa täysin samaan osoitteeseen täysin samoilla kriteereillä. Kuviossa 3 käydään läpi pakettipohjainen prosessi siitä lähtien, kun paketti saapuu laitteeseen. Kun paketti tulee sisääntulorajapintaan (ingress interface), paketti käy läpi tilattomat palomuurisuodattimet (stateless firewall filters) ja palveluntason (Class of Service), ennen kuin määritellään ulospäin lähtevä rajapinta (egress interface) kohdassa *route lookup*. Kun ulkorajapinta on selvitetty, paketti käy jälleen läpi määritellyt suodattimet ja tämän jälkeen lähetetään ulkorajapintaan, josta se lähetetään eteenpäin. (Juniper Networks Security Configuration Guide 2011, 96)



KUVIO 3. Pakettipohjainen prosessi
(Juniper Networks Security Configuration Guide 2011, 94)

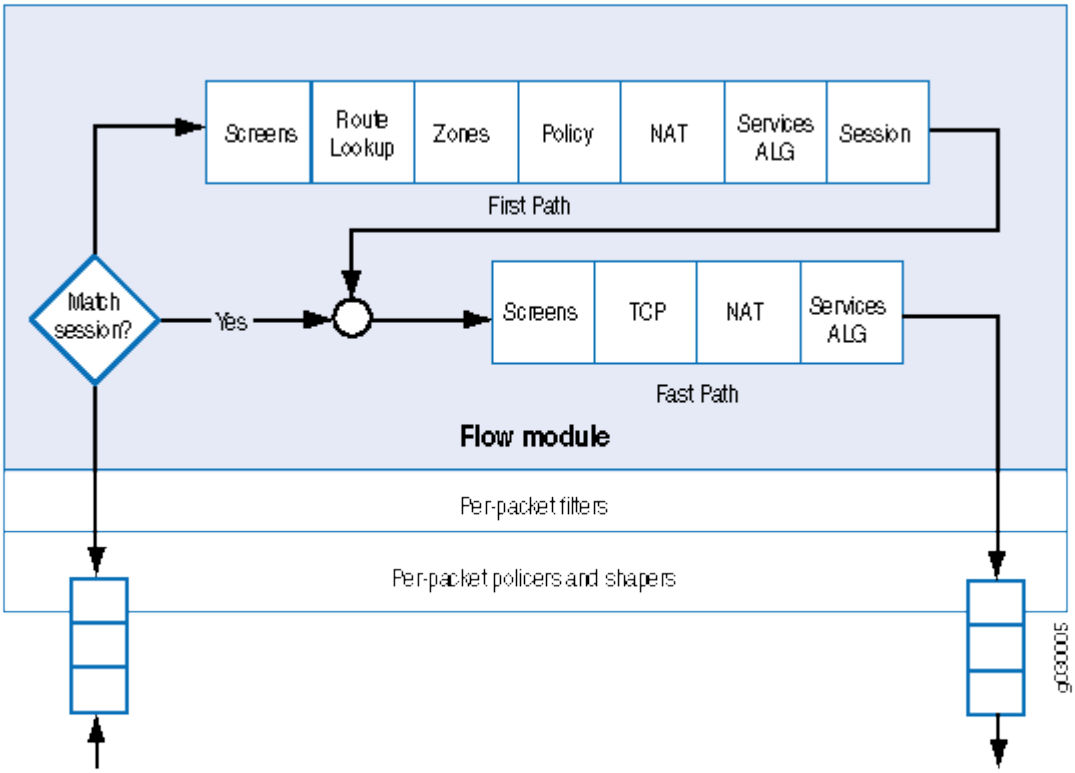
4.1.3 Vuopohjainen prosessointi

Pakettivuo on useammasta paketista muodostuva pakettivirta. Kun paketti saapuu järjestelmään, sitä kohdellaan ensin pakettipohjaisesti. Järjestelmä asettaa suodattimet (Firewall Filters) ja palveluntason (CoS) luokittelut paketille, jonka jälkeen järjestel-

mä tarkistaa, kuuluuko paketti jo olemassa oleviin istuntoihin. Järjestelmä käyttää kuutta eri tarkistuskriteeriä:

1. Istunnon tunnus
2. Lähdeosoite
3. Kohdeosoite
4. Lähdeportti
5. Kohdeportti
6. Protokolla.

Jos paketti vastaa istunnon kriteereitä, käytetään ns. nopean polun prosessointia (Fast-Path Processing). Mikäli paketti ei vastaa olemassa olevien istuntojen kriteereitä, käytetään ensimmäisen paketin prosessointia (first-packet processing), jossa luodaan uusi istunto ensimmäisen paketin tietoturvaominaisuuksien perusteella. (Ks. kuvio 4.) (Juniper Networks Security Configuration Guide 2011, 104)



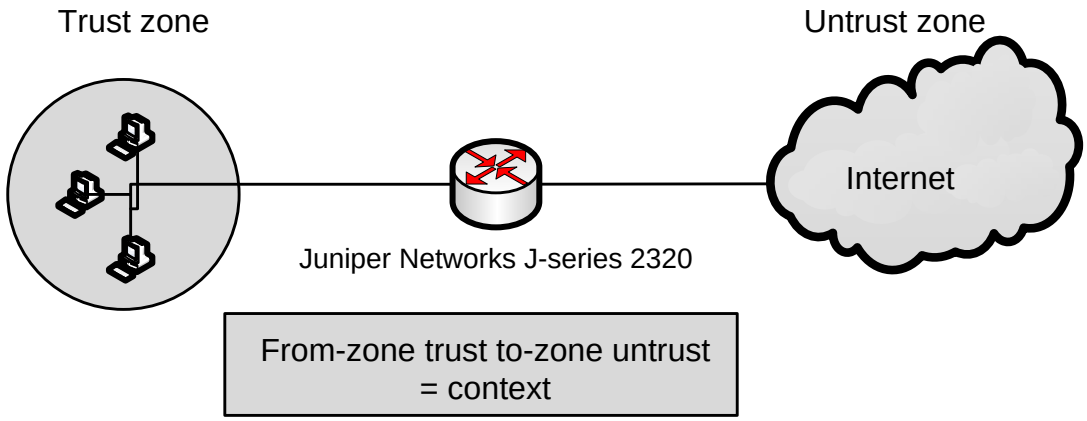
KUVIO 4. Vuopohjainen prosessointi

(Juniper Networks Security Configuration Guide 2011, 104)

4.2 Turva-alue (Security Zone)

4.2.1 Yleistä

Turva-alue on yhdestä tai useammasta verkon osasta tehty kokonaisuus, johon yksi tai useampi rajapinta on sidoksissa. Yhteen reitittimeen on mahdollista luoda useita turva-alueita tarpeen mukaan, mutta vähintään kaksi turva-aluetta on pakko luoda: sisään tulevan liikenteen alue ja ulosmenevän liikenteen alue. Turva-alueiden tarkoitus on rajoittaa ja monitoroida verkon liikennettä jakamalla verkko osiin. Liikenne turva-alueiden välillä toimii *from-zone to-zone* periaatteella (ks. kuvio 5). Tätä *from-zone to-zone* -yhdistelmää kutsutaan sanalla konteksti (context). Jokainen konteksti sisältää järjestelmällisen listan sääntöjä (policy), jotka määrittelevät tarkemmin liikenteen rajoitteista ja monitoroinnista. (Juniper Networks Security Configuration Guide 2011, 109–111)



KUVIO 5. Konteksti

4.2.2 Sisään tulevan liikenteen rajaaminen (Host inbound traffic)

Turva-alueisiin on mahdollista määritellä suoraan rajapinnoissa kiinni olevista laitteista tulevien palvelujen ja protokollien yhteyksiä. Sisään tulevaa liikennettä on mahdollista rajata turva-alueen tai rajapinnan tasolla. Turva-alueiden tasolla tehdyt määritykset vaikuttavat alueen kaikkiin sidoksissa oleviin rajapintoihin, kun taas pelkästään rajapintaan tehdyt muutokset koskevat vain kyseistä rajapintaa. (Juniper Networks Security Configuration Guide 2011, 114)

Yleisin käyttötapa on kieltää telnet palvelun käyttö. Telnet palvelun kieltäminen suojaa verkkoa hyökkäyksiltä, jotka tehdään fyysisesti rajapinnassa kiinni olevilla laitteilla. Laitteen alkuperäisasetuksissa kaikki palvelut ovat automaattisesti poissa käytöstä. Kuvioista 6 ja 7 selviävät määriteltävät palvelut ja protokollat

Host Inbound System Services	
all	any-service
dns	finger
ftp	http
https	indent-reset
ike	netconf
ntp	ping
reverse-ssh	reverse-telnet
rlogin	rpm
rsh	sip
snmp	snmp-trap
ssh	telnet
tftp	traceroute
xnm-clear-text	xnm-ssl

KUVIO 6. Lista palveluita, joita on mahdollista rajata.

(Juniper Networks Security Configuration Guide 2011, 115)

Protocols	
all	bfd
bgp	dvmrp
igmp	msdp
ndp	nhrp
ospf	ospf3
pgm	pim
rip	ripng
sap	vrrp

KUVIO 7. Lista protokollista, joita on mahdollista rajata
(Juniper Networks Security Configuration Guide 2011, 116)

4.2.3 Osoitekirjat ja osoiteryhmät

Jokaisella turva-alueella on oma osoitekirja (address book). Ennen kuin turvasääntöjä voidaan määritellä, on molemmille turva-alueille määriteltävä osoitekirjat. Mikäli turva-alueessa on useita osoitekirjoja, on niistä mahdollista tehdä osoiteryhmiä (address sets). Osoite, joka lisätään osoitekirjaan voi sisältää minkä tahansa yhdistelmän IPv4 osoitteita, IPv6-osoitteita, wildcard -osoitteita ja Domain Name Server (DNS) -nimiä. Osoitteelle annetaan uniikki nimi, ja se ei saa olla sama kuin osoiteryhmällä. Myöhemmin turvasääntöjä muodostettaessa ei siis enää viitata IP-osoitteisiin, vaan osoitekirjoihin tai osoiteryhmiin. (Juniper Networks Security Configuration Guide 2011, 132-133.)

4.2.4 Application Layer Gateway (ALG)

Juniper Systemsin J-series reitittimissä on ominaisuus nimeltä Application Layer Gateway (ALG), jolla hallitaan protokollia, kuten File Transfer Protocol (FTP). ALG:n voi aktivoida joko palvelu tai sovellus, joka on konfiguroituna turva-alueen sääntöihin (Security Policy). Tässä tapauksessa palvelu on OSI-mallin kerroksella neljä toimiva protokolla kuten Transmission Control Protocol (TCP) tai User Datagram Protocol (UDP). Sovellus tarkoittaa OSI-mallin kerroksella seitsemän toimivia sovelluksia,

jotka vaativat kerroksen neljä palveluita toimiakseen. (Juniper Networks Security Configuration Guide 2011, 201 – 202.)

ALG on vastuussa OSI-mallin kerroksen seitsemän sovellusten tietoisesta pakettien prosessoinnista. ALG analysoi määritetyn liikenteen, allokoi resurssit ja määrittelee dynaamiset säännöt, joilla sallitaan liikenne turvallisesti laitteen läpi. ALG:ssä on ennalta määritettyjä palveluita, joihin ovat sidoksissa tietyt sovellukset. Jos haluttua palvelua ei ole ennalta määritetty, se on määriteltävä erikseen. (Juniper Networks Security Configuration Guide 2011, 201 – 202.)

4.3 Turvasäännöt (Security Policy)

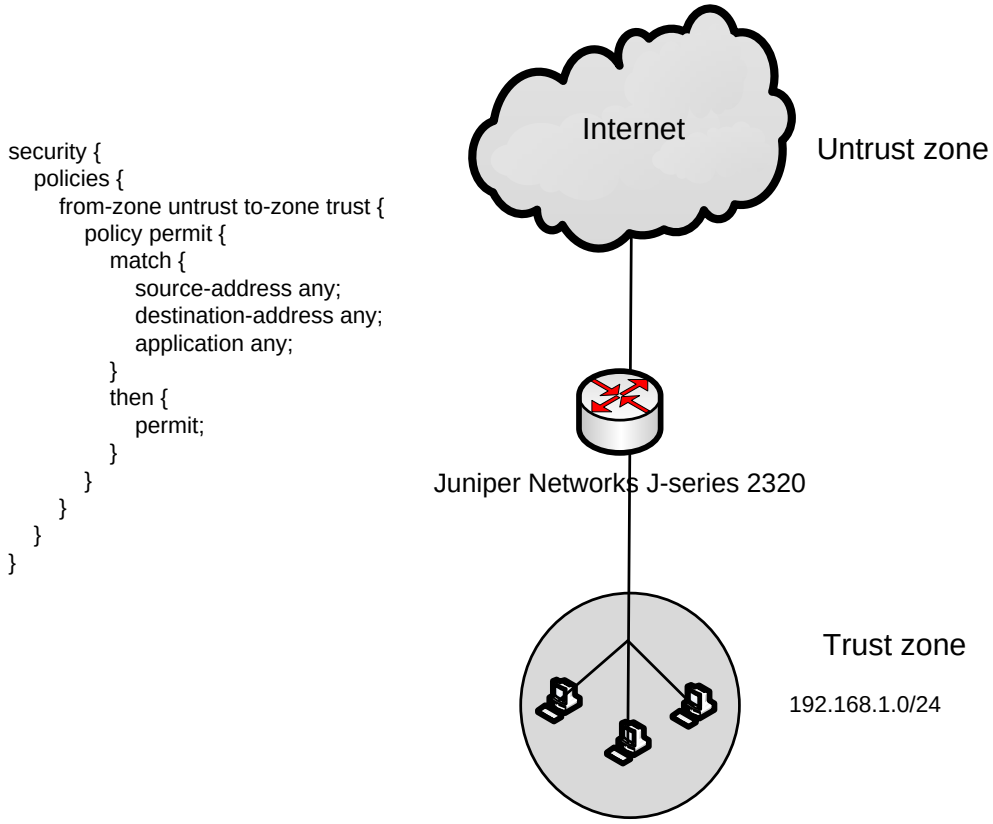
4.3.1 Yleistä

Junos-käyttöjärjestelmän tilallisessa palomuurissa on mahdollista määritellä sääntöjä tiedonsiirrolle. Säännöt määrittelevät, mitkä yhteydet pääsevät palomuurista läpi ja mitä tiedonsiirrolle siinä yhteydessä tehdään. Säännöt sijoittuvat tiedonsiirrossa siten, että dataliikenne etenee turva-alueesta toiseen *from-zone to-zone* periaatteella muodostaen kontekstin. Jokainen konteksti sisältää järjestelmällisen listan sääntöjä, jotka käydään läpi järjestyksessä. Säännöt hallitsevat liikennettä turva-alueesta toiseen määrittelemällä sallitun liikenteen lähdeosoitteen, kohdeosoitteen ja sovelluksen mukaan. Säännöillä on mahdollista määrittää seuraavat toimenpiteet tiedonsiirrolle:

- Deny – kieltää tiedonsiirto
- Permit – sallia tiedonsiirto
- Reject – estää tiedonsiirto (eroaa kiellosta siten, että paketin pudottamisen sijaan lähettää lähdeosoitteelle TCP RST- tai ICMP port unreachable viestin.)
- Encrypt – salata tiedonsiirto
- Decrypt – purkaa salattu tiedonsiirto
- Authenticate – varmentaa tiedonsiirron alkuperän aitous
- Prioritize – priorisoida tiedonsiirtoa
- Schedule – aikatauluttaa tiedonsiirtoa
- Filter – suodattaa tiedonsiirtoa
- Monitor – monitoroida tiedonsiirtoa

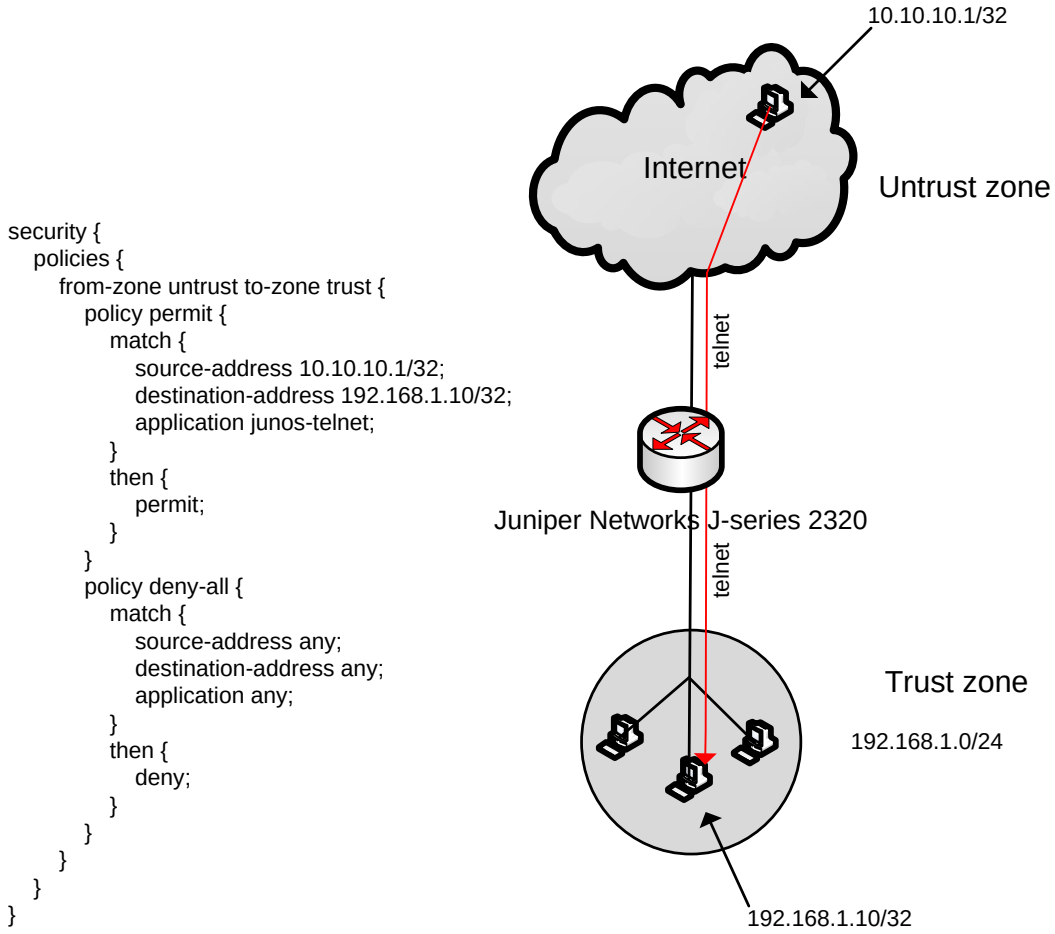
Sääntöjä luomalla, on väljimmillään mahdollista sallia kaikki liikenne kaikista suunnista ilman mitään aikarajoitteita ja tiukimmillaan sallitaan liikenne vain tietystä lähdeosoitteesta, määritettyyn kohdeosoitteeseen, ennalta määritellystä ohjelmasta tiettyyn aikaan. (Juniper Networks Security Configuration Guide 2011, 143 – 145.)

Kuviossa 8 on esimerkki säännöstä, jolla sallitaan kaikki liikenne turva-alueesta *Untrust*, turva-alueeseen *Trust*.



KUVIO 8. Sääntö, jossa kaikki liikenne sallitaan turva-alueiden välillä

Kuviossa 9 on esimerkkinä sääntö, joilla sallitaan pelkästään telnet yhteys turva-alueen *untrust* osoitteesta 10.10.10.1/32 kohdeosoitteeseen 192.168.1.10/32 turva-alueessa *trust*.



KUVIO 9. Sääntö, jolla sallitaan vain telnet yhteys.

4.3.2 Ominaisuudet

Jokainen sääntö on uniikki nimeltään. Liikenne luokitellaan tarkastelemalla tiedonsiirron lähde- ja kohde turva-alueet, lähde- ja kohdeosoitteet ja ohjelmat. Jokaisella säännöllä on mahdollista olla seuraavanlaiset kriteerit, millä liikenne tunnistetaan:

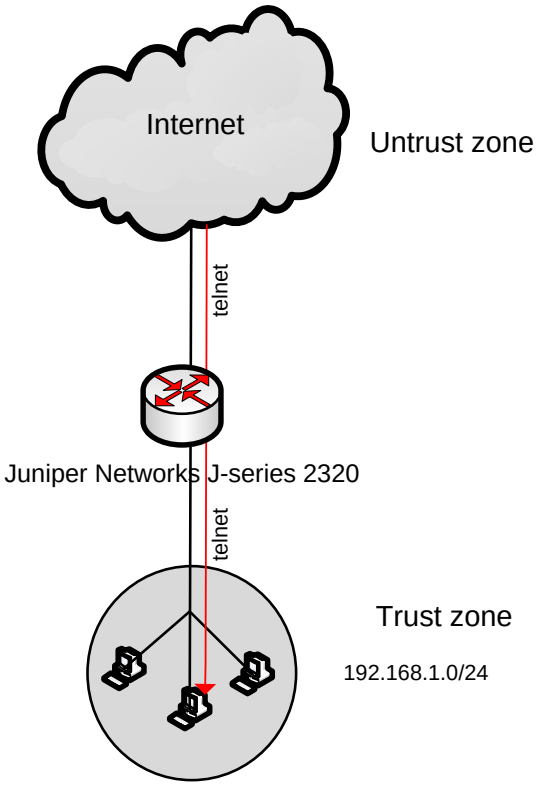
- Lähdeosoite
- Kohdeosoite
- Yksi tai useampi lähdeosoitteen osoitekirjan nimi tai osoiteryhmän nimi
- Yksi tai useampi kohdeosoitteen osoitekirjan tai -ryhmän nimi
- Yksi tai useampia sovelluksen nimiä tai sovellusryhmien nimiä

Jokaisella säännöllä on myös tietty toimenpide, mitä se liikenteelle tekee, kun oikeat kriteerit löytyvät. Säännölle ei ole välttämättä pakko määritellä tarkkaa kriteeriä esim. lähdeosoitteelle, jos halutaan lähdeosoitteeksi kaikki mahdolliset osoitteet. Tässä ta-

pauksessa laitetaan varsinaisen osoitteen kohdalle *any*. Kun tiedonsiirto menee kontekstin läpi, käy se läpi kaikki säännöt järjestyksessä ylhäältä alas. Mikäli vastaavuuksia ei löydy, paketit pudotetaan pois. Kun liikenne kohtaa ensimmäisen säännön, jossa tiedonsiirto vastaa sääntöön määritettyjä kriteereitä, toteutetaan säännössä määritetty toiminta ja loppuja sääntöjä ei käydä enää läpi. On siis erittäin tärkeätä, että yksityiskohtaiset säännöt ovat listan alkupäässä ja kaikista väljimmät säännöt listan loppupuolella. (Juniper Networks Security Configuration Guide 2011, 146.)

Kuviossa 10 on esimerkki sääntöjen järjestelyn tärkeydestä. Esimerkissä on kaksi sääntöä: *permit* ja *deny-telnet*. *Permit* säännössä sallitaan kaikki liikenne *untrust* turva-alueesta *trust* turva-alueen aliverkkoon 192.168.1.0/24 ja *deny-telnet* säännössä kielletään telnet yhteydet *untrust* turva-alueesta *trust* turva-alueen samaiseen aliverkkoon. Koska sääntö *permit* on listassa ensimmäisenä, jää *deny-telnet* sääntö täysin huomioimatta ja telnet yhteydet sallitaan.

```
security {
    policies {
        from-zone untrust to-zone trust {
            policy permit {
                match {
                    source-address any;
                    destination-address 192.168.1.0/24;
                    application any;
                }
                then {
                    permit;
                }
            }
            policy deny-telnet {
                match {
                    source-address any;
                    destination-address 192.168.1.0/24;
                    application junos-telnet;
                }
                then {
                    deny;
                }
            }
        }
    }
}
```



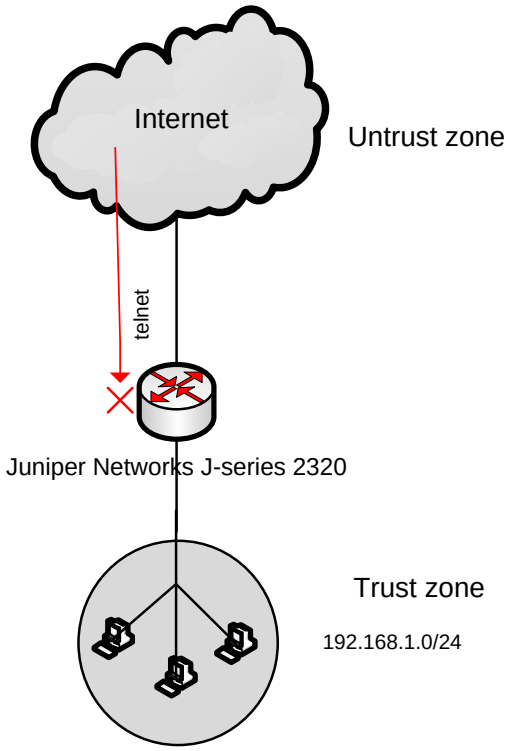
KUVIO 10. Sääntöjen järjestyksen merkitys

Sääntöjen järjestystä on mahdollista muuttaa jälkikäteen. Kuvion 10 mukainen konfiguraatio saadaan korjattua siirtämällä sääntö *permit* säännön *deny-telnet* jälkeen. Tämä tapahtuu komennolla:

user@host# insert security policies from-zone untrust to-zone trust policy deny-telnet before policy permit

Nyt sääntö *deny-telnet* käydään läpi ensiksi, joten telnet yhteyksiä aliverkkoon 192.168.1.0/24 ei hyväksytä, mutta muu liikenne pääsee liikkumaan vapaasti (ks. kuvio 11).

```
security {
    policies {
        from-zone untrust to-zone trust {
            policy deny-telnet {
                match {
                    source-address any;
                    destination-address 192.168.1.0/24;
                    application junos-telnet;
                }
                then {
                    deny;
                }
    }
    policy permit {
                match {
                    source-address any;
                    destination-address 192.168.1.0/24;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
    }
}
```



KUVIO 11. Sääntö deny-telnet

4.3.3 Ajastus

Yleensä säännöt määritetään toimintaan jatkuvaksi, ilman aikarajoitteita. On kuitenkin mahdollista aktivoida tietty sääntö vain ennalta määrätylle ajalle. Ajastimen (scheduler) voi määrittää yksittäisesti yhdelle ajalle tai toistuvana esimerkiksi joka päivä klo. 08:00 – 16.00. Kun ajastin ei ole enää aktiivinen, siihen liitetty sääntö poistuu listalta ja kaikki kyseisessä säännössä määritetyt sessiot katkaistaan. (Juniper Networks Security Configuration Guide 2011, 165.)

4.4 Network Address Translation (NAT)

4.4.1 Yleistä

Network Address Translation luotiin ratkaisemaan IPv4-osoitteiden loppuminen. Tämän jälkeen NAT on ollut käytännöllinen työkalu palomuureille. NAT voi muokata tai muuttaa verkon osoitetietoja paketin kehyksestä. Joko kohde- tai lähdeosoitteet on mahdollista muuttaa tai peräti molemmat. NAT mahdollistaa IP-osoitteiden muokkauksen lisäksi myös porttien numeroiden muokkauksen. Juniper Networksin laitteet tukevat kolmea NAT tyyppiä, jotka ovat staattinen NAT, kohde NAT ja lähde NAT. (Juniper Networks Security Configuration Guide 2011, 1199.)

4.4.2 NAT säännöt ja sääntöryhmät

NAT toimii sääntöryhmien avulla. Staattisessa ja kohde NAT:ssa sääntöryhmä määrittelevät yhden seuraavista:

- Kohteen rajapinta
- Kohteen turva-alue
- Kohteen reititys instanssi (routing-instance)

Lähde NAT:ssa sääntöryhmään määritellään molemmat, kohteen ja lähteen ominaisuudet eli rajapinnat, turva-alueet ja reititys instanssit. (Juniper Networks Security Configuration Guide 2011, 1200 - 1202.)

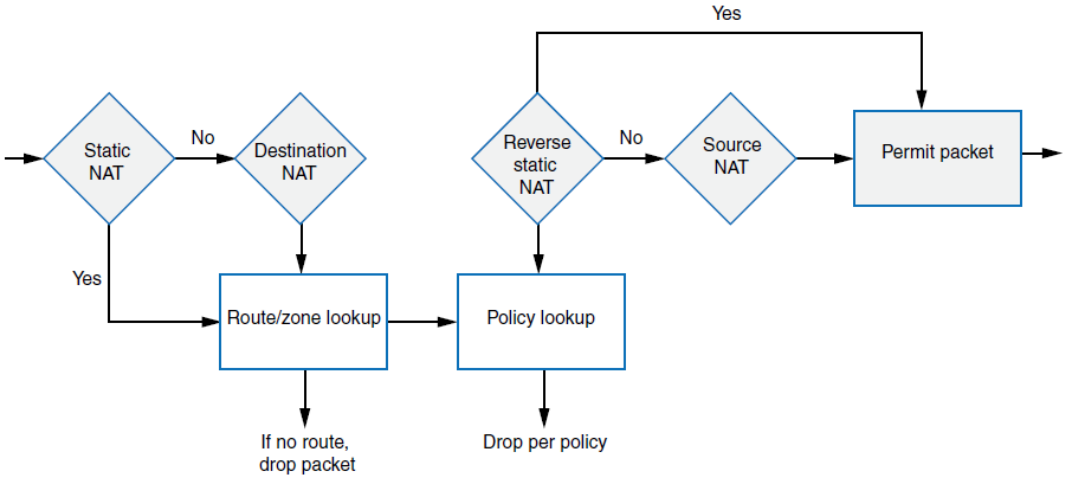
Kun liikenteelle löytyy vastaava sääntöryhmä, jokainen sääntö sääntöryhmän sisällä arvioidaan ja tarkistetaan löytyykö vastaavuuksia. NAT säännöt sisältävät seuraavia parametrejä:

- Kohde osoite (vain staattisessa NAT:ssa)
- Lähde ja kohde osoitteet (kohde ja lähde NAT)
- Kohde portti (kohde ja lähde NAT)

Kun liikenteelle löytyy vastaavuus säännöistä, ensimmäistä sääntöä käytetään ja liikenne prosessoidaan säännön määräämällä tavalla. NAT tyyppi määrittelee järjestyksen, miten NAT säännöt prosessoidaan. Pakettivuon ensimmäisen paketin prosessoinnissa NAT säännöt laitetaan käytäntöön seuraavassa järjestyksessä (ks. kuvio 12):

1. Staattisen NAT:n säännöt
2. Kohde NAT:n säännöt
3. Reitin selvitys
4. Tietoturva säännöt (Security Policy lookup)
5. Käänteisen staattisen NAT:n säännöt
6. Lähde NAT:n säännöt.

(Juniper Networks Security Configuration Guide 2011, 1200 - 1202.)



KUVIO 12. NAT sääntöjen prosessointi

(Juniper Networks Security Configuration Guide 2011, 1202)

4.4.3 Staattinen NAT (Static NAT)

Staattinen NAT määrittelee yksi-yhteen osoitteenmuutoksen yhdestä aliverkosta toiseen. Tämä sisältää kohde IP-osoitteen muuntamisen yhteen suuntaan ja lähde IP-osoitteen muuntamisen toiseen suuntaan. NAT laitteesta päin katsoen, alkuperäinen kohdeosoite on virtuaalisen käyttäjän IP-osoite ja muunnettu osoite on oikea IP-osoite. Staattinen NAT sallii yhteyksiä verkon molemmilta puolilta, mutta osoitteen muunta-

minen on rajoitettu yhden yksityisen osoitteen muuntamisen julkiseksi osoitteeksi tai aliverkon muuntamisen samankokoiseen aliverkkoon. Jokaiselle yksityiselle IP-osoitteelle on määriteltävä yleinen IP-osoite ja jokaiselle yksityiselle aliverkolle on määriteltävä yleinen samankokoinen aliverkko. (Juniper Networks Security Configuration Guide 2011, 1203.)

4.4.4 Kohde NAT (Destination NAT)

Kohde NAT muuttaa kohteen IP-osoitteen toiseksi IP-osoitteeksi. Esimerkiksi uudelleenohjataan liikenne, joka on tarkoitettu virtuaaliselle käyttäjälle (alkuperäinen IP-osoite), menemään oikealle käyttäjälle (muutettu IP-osoite). Kohde NAT sallii yhteyksiä vain sisään tuleville yhteyksille, esimerkiksi Internetistä yksityiseen verkkoon. IP-osoitteen muuntamisen lisäksi kohde NAT:lla on mahdollista muuntaa myös porttinumeroita. (Juniper Networks Security Configuration Guide 2011, 1214 – 1215.)

4.4.5 Lähde NAT (Source NAT)

Lähde NAT:lla muunnetaan lähde IP-osoite toiseen IP-osoitteeseen ja se sallii yhteyksien aloituksen vain ulospäin suuntautuville yhteyksille. Lähde NAT:n yleisin käyttötarkoitus on sallia yksityisen IP-aliverkon pääsy Internetiin. Lähde NAT:lla on mahdollista muuttaa myös porttinumeroita. (Juniper Networks Security Configuration Guide 2011, 1233.)

5 Intrusion Detection and Prevention (IDP)

5.1 Käyttötarkoitus

Juniperin Intrusion Detection and Prevention (IDP) ominaisuus havaitsee ja estää verkkoa kohti tehtyjä hyökkäyksiä. Hyökkäys voi olla joko informaatiota keräävä isku tai hyökkäys jossa estetään tai vahingoitetaan verkon toimintaa. Joissain tapauksissa hyökkäyksen tapa voi olla epäselvä. Esimerkiksi TCP SYN segmenttien ryöppy voi olla IP address sweep, jossa kalastellaan vastauksia aktiivisilta käyttäjiltä tai se voi olla SYN flood -hyökkäys, jolla yritetään tukkia verkko käyttökelvottomaksi. Yleensä hyökkääjä selvittää ensin verkon heikot kohdat muutamalla informaatiota keräävällä iskulla, jonka jälkeen tapahtuu vasta hyökkäys, jolla vahingoitetaan verkon toimivuutta. Tämän takia myös informaatiota keräävät iskut ovat luokiteltu hyökkäyksiksi tai paremminkin esihyökkäyksiksi. (Juniper Networks Security Configuration Guide 2011, 899 – 900.)

Näitä hyökkäyksiä on mahdollista estää Screenien avulla. Screenit toimivat turva-alueiden tasolla eli jokainen Screen on sidottava turva-alueeseen, jos se halutaan aktivoida. Screenit toimivat siten, että ne ensin tutkivat liikenteen, joka haluaa päästä turva-alueesta toiseen ja tämän jälkeen joko sallii tai kieltää liikenteen. (Juniper Networks Security Configuration Guide 2011, 899 – 900.)

Seuraavissa kappaleissa käydään läpi esimerkkejä eri hyökkäystavoista ja Screeneistä, joilla hyökkäykset estetään Junos käyttöjärjestelmässä.

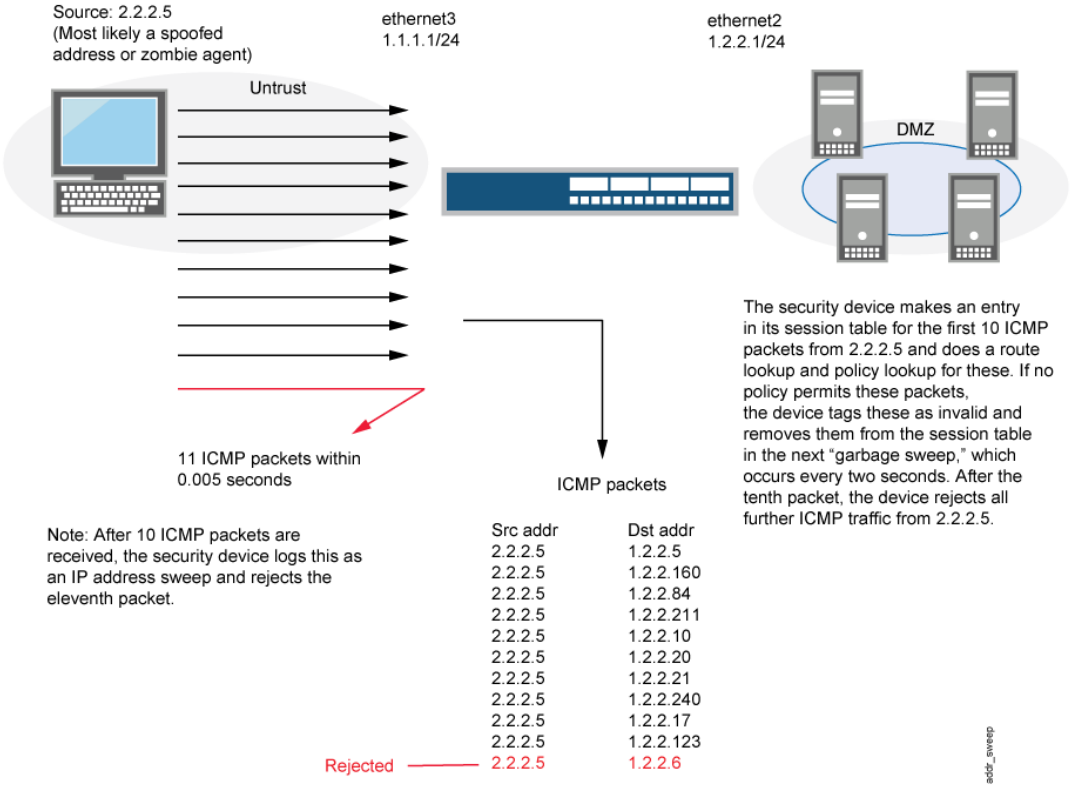
5.2 Tiedusteluhyökkäykset

5.2.1 Yleistä

Tiedusteluhyökkäys tapahtuu yleensä suunnitteluvaiheessa, eli hyökkääjä haluaa saada selville kohdeverkon heikot kohdat. Näillä tiedusteluhyökkäyksillä on mahdollista selvittää mm. IP-osoitteita, avoimia portteja ja kohteiden käyttöjärjestelmiä. (Juniper Networks Security Configuration Guide 2011, 901.)

5.2.2 IP-osoitteiden selvitys

IP-osoitteiden selvitys (IP address sweep) tapahtuu siten, että yhdestä lähdeosoitteesta lähetetään tietty määrä ICMP paketteja eri vastaanottajille. Jos vastaanottaja vastaa ICMP-pakettiin, on vastaanottajan IP-osoite selvillä. Jos käyttöjärjestelmän Screen nimeltä ip-sweep on aktivoituna, Junos käyttöjärjestelmä itsenäisesti laskee ICMP pakettien määrän, jotka lähtevät samasta osoitteesta, mutta kohde vaihtuu kokoajan. Perusasetuksilla riittää, että lähdeosoitteesta tulee kymmenen ICMP-pakettia 0,005 sekuntin sisällä, jonka jälkeen laite estää kaikki tulevat ICMP paketit kyseisestä osoitteesta (ks. kuvio 13). (Juniper Networks Security Configuration Guide 2011, 901 – 902.)



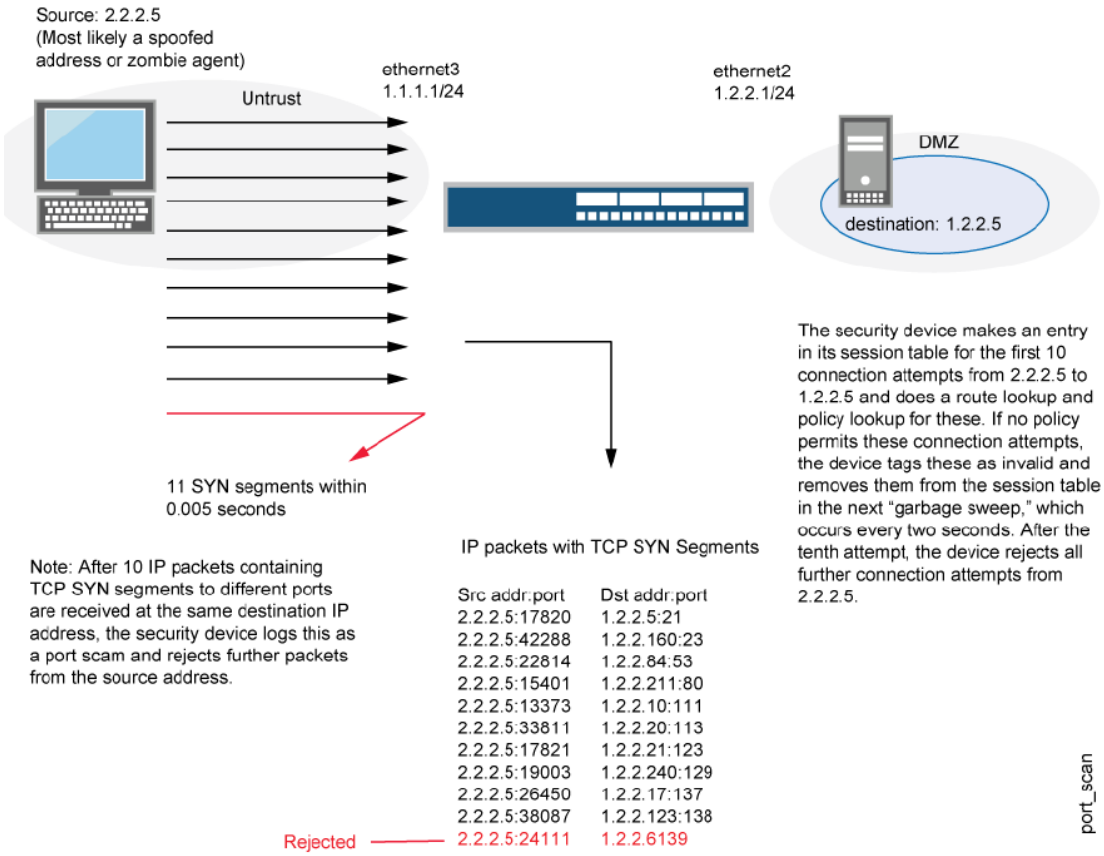
KUVIO 13. Screen ip-sweep

(Juniper Networks Security Configuration Guide 2011, 902)

5.2.3 Porttiskannaus

Porttiskannauksessa lähetetään yhdestä lähdeosoitteesta TCP SYN paketteja kohdeosoitteeseen eri porteilla. Tavoitteena on selvittää, mitkä portit vastaavat kyseiseen pakettiin, jolloin käytettävät palvelut selviävät hyökkääjälle. Junos-käyttöjärjestelmän Screen *port-scan*, estää porttiskannauksen laskemalla samasta osoitteesta tehdyt eri

portteihin kohdistuneet skannaukset. Kun 10 porttia on skannattu 0,005 sekunnin sisällä, järjestelmä merkitsee tämän porttiskannaus hyökkäykseksi ja estää tulevat paketit kyseisestä osoitteesta (ks. kuvio 14). (Juniper Networks Security Configuration Guide 2011, 904 – 905.)



KUVIO 14. Port-scan Screen

(Juniper Networks Security Configuration Guide 2011, 904 – 905)

5.2.4 Käyttöjärjestelmän tiedustelu

Ennen virallista hyökkäystä, hyökkääjä voi yrittää tiedustella, mikä on kohteessa käytettävä käyttöjärjestelmä, jotta hyökkäyksen tyyppi voitaisiin määritellä tarkemmin. Käyttöjärjestelmän tiedusteluhyökkäykset tehdään lähettämällä TCP-paketteja, joiden otsikkotietoja on muokattu sisältämään esimerkiksi SYN ja FIN merkintäliput, jolloin vastaanottajalta saadaan erilaisia vastauksia käyttöjärjestelmästä riippuen. Koska yleensä TCP-paketissa ei kuulu olla molempia merkintälippuja, Junos käyttöjärjestelmä tulkitsee tämän tiedusteluhyökkäykseksi, jos Screen TCP SYN FIN on aktivoituna. (Juniper Networks Security Configuration Guide 2011, 912 – 913.)

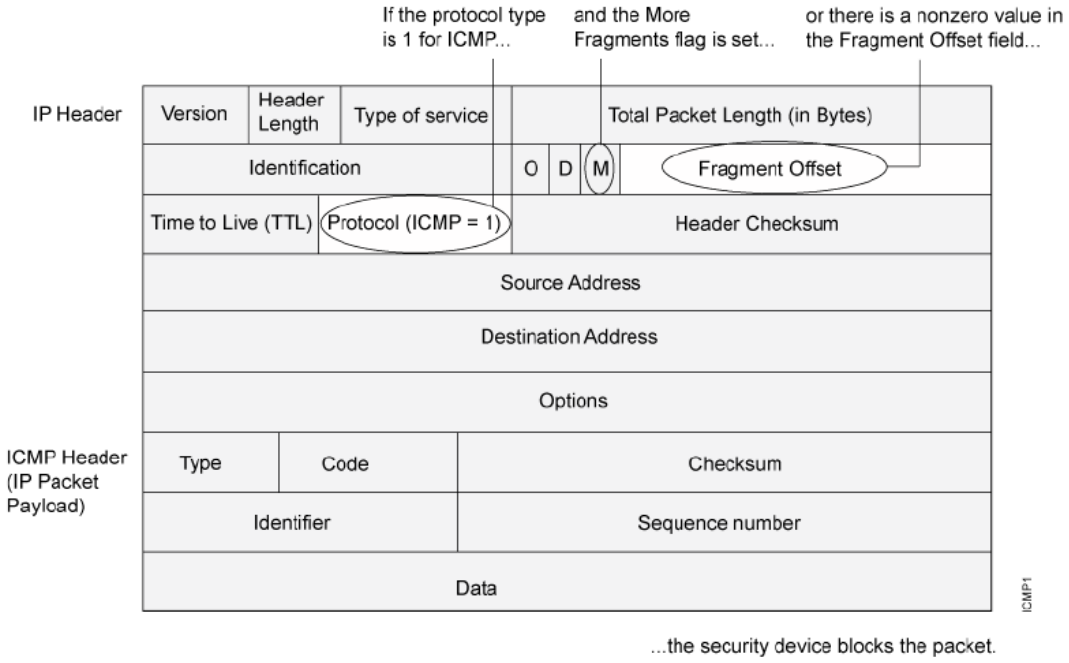
5.3 Epäilyttävät paketit

5.3.1 Yleistä

Joskus paketti voi olla tarkoitettu tiedustelua varten tai laukaista isku verkkoa vastaan ja joskus on epäselvää, mikä paketin lopullinen tarkoitus on. Jos paketin IP-options asetuksia tai ICMP-paketin kokoa on muutettu ylisuureksi, lasketaan nämä epäilyttävien pakettien hyökkäyksiksi.

5.3.2 Fragmentoitunut ICMP-paketti

Koska Internet Control Message Protocol (ICMP) virheen ja verkon tutkimisviestit ovat niin lyhyitä, ei sillä ole syytä olla fragmentoitunut. Jos ICMP-paketti on niin iso, että sen on täytynyt fragmentoitua, on jotain vialla. Kun Junos käyttöjärjestelmän Screen *icmp-fragment* on aktivoituna, tarkistaa järjestelmä ICMP pakettien otsikkotiedoista, onko More Fragment -kohta aktivoituna sekä onko arvo kohdassa Fragment Offset joku muu kuin 0. (Ks. kuvio 15.) (Juniper Networks Security Configuration Guide 2011, 934.)

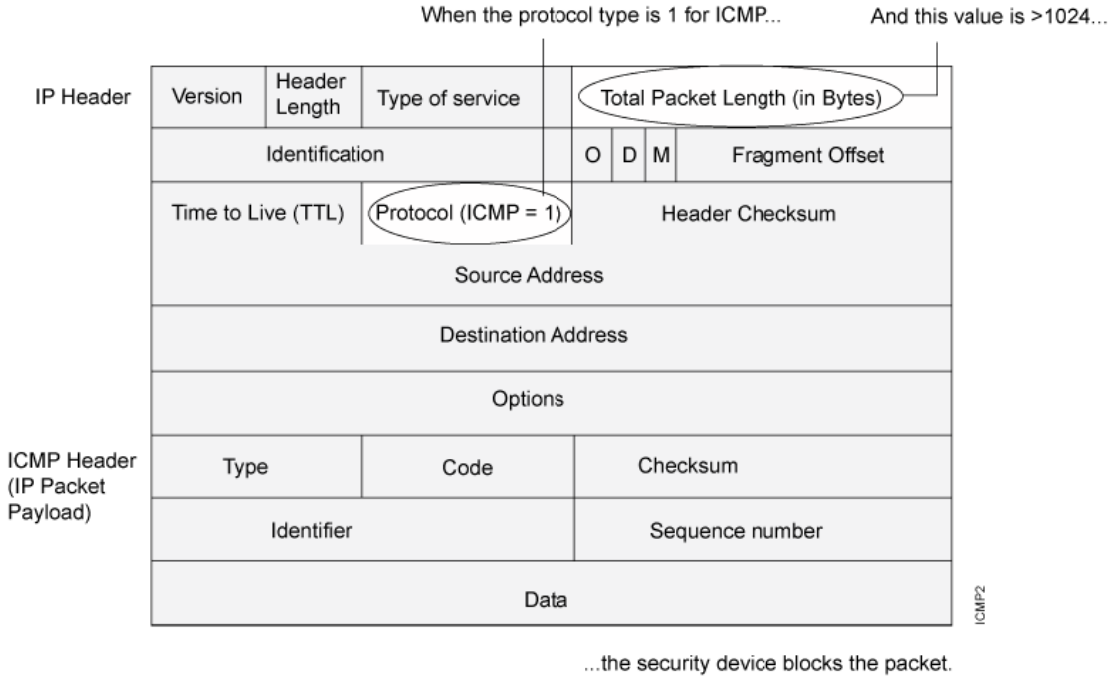


KUVIO 15. Fragmentoitunut ICMP paketti

(Juniper Networks Security Configuration Guide 2011, 934)

5.3.3 Ylisuuri ICMP-paketti

Jos ICMP-paketti on liian suuri, on yleensä jotain kyseenalaista toimintaa tapahtumassa. Junos käyttöjärjestelmän Screen *icmp-large* estää liian suuret ICMP-paketit tarkistamalla IP-osoitteen otsikkokentästä kohdan Total Packet Length. Jos arvo on yli 1024, on paketti liian suuri ja Junos-käyttöjärjestelmä hylkää paketin. (Ks. Kuvio 16.) (Juniper Networks Security Configuration Guide 2011, 936.)

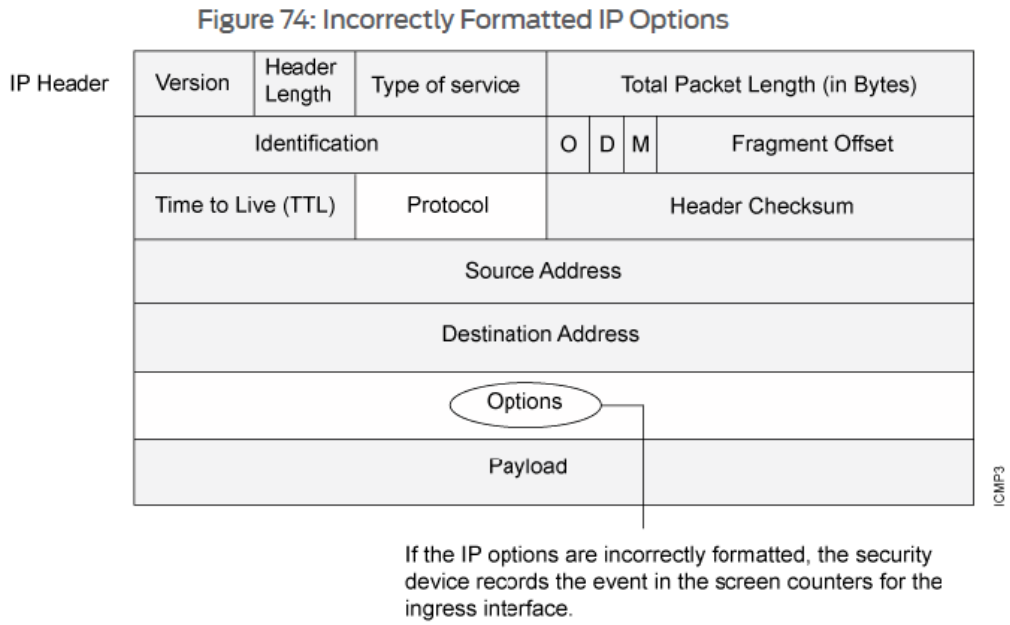


KUVIO 16. Icmp-large Screen

(Juniper Networks Security Configuration Guide 2011, 936)

5.3.4 Väärä IP protokollan asetusarvo (IP Options)

IP-protokollassa on kahdeksan asetusta, joilla on mahdollista konfiguroida erikoisia reititysvalintoja, virheenmääritystyökaluja sekä tietoturvaominaisuuksia. Vaikka nämä asetukset ovat alunperin suunniteltu hyvin tarkoitusperin, on niitä mahdollista käyttää myös vääriin tarkoituksiin.. Junos-käyttöjärjestelmän Screen *ip-bad-option* (ks. kuvio 17) suojaa laitteistoa näiltä väärinkäytöksiltä tarkistamalla IP-kehyksen *Options* -kentän. Jos tämä asetuskenttä on väärässä formaatissa, paketti blokataan. (Ks. kuvio 17.) (Juniper Networks Security Configuration Guide 2011, 937.)

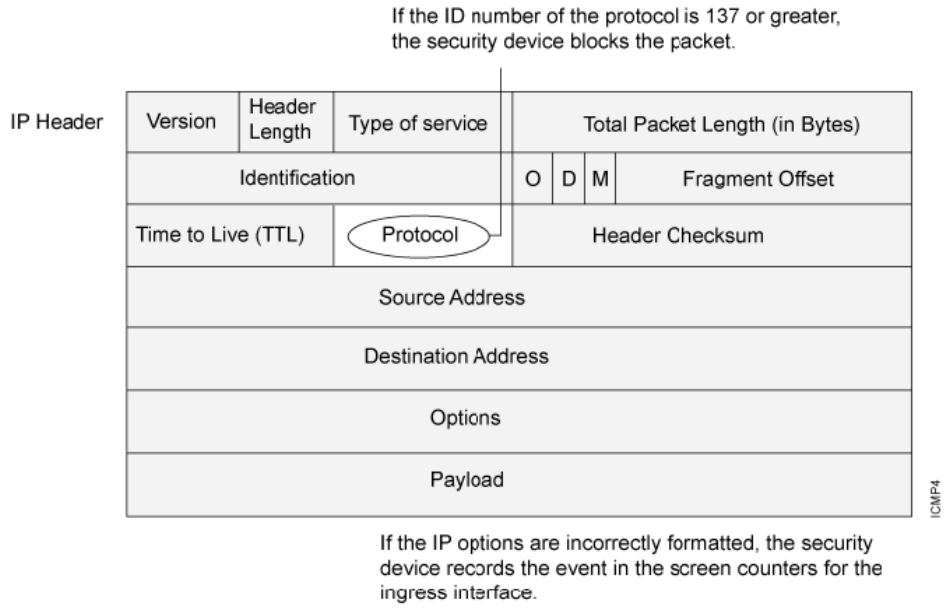


KUVIO 17. Väärä IP-asetus

(Juniper Networks Security Configuration Guide 2011, 936 – 938)

5.3.5 Tuntematon protokolla Screen

Tällä hetkellä protokollien ID:t 137. ylöspäin on varattu ja määrittelemättömiä. Tästä johtuen Junos käyttöjärjestelmän Screen *unknown-protocol* tarkistaa IP-kehyksestä protokolla numeron ja jos ID on yli 137, paketti estetään (Ks. kuvio 18). (Juniper Networks Security Configuration Guide 2011, 939 – 940.)

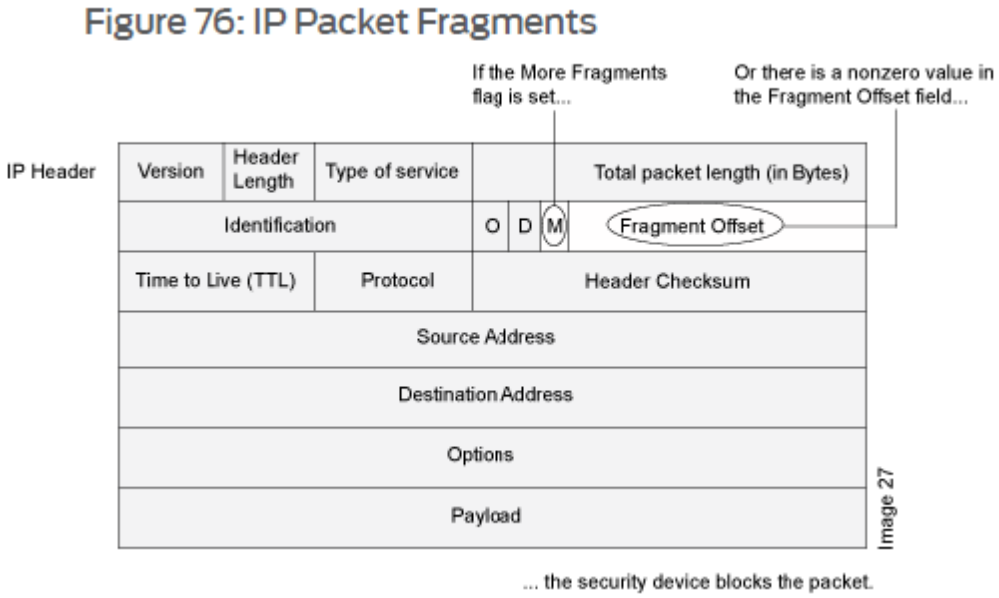


KUVIO 18. Tuntemattomat protokollat –Screen

(Juniper Networks Security Configuration Guide 2011, 940)

5.3.6 Fragmentoituneet IP-paketit

Kun paketit liikkuvat verkossa, on joskus välttämätöntä hajottaa paketti pienempiin osiin. IP-paketin osat voi olla hyökkääjän yritys käyttää paketin uudelleenrakennuskoodia hyväkseen, joten Junos käyttöjärjestelmän Screen *ip block-frag* estää fragmentoituneet IP-paketit. (Ks. Kuvio 19). (Juniper Networks Security Configuration Guide 2011, 941.)



KUVIO 19. Fragmentoituneen IP-paketin Screen
(Juniper Networks Security Configuration Guide 2011, 942)

5.3.7 Fragmentoituneet TCP SYN segmentit

IP sisältää TCP SYN segmentin IP-paketissa, joka ehdottaa TCP-yhteyden luomista. Hyökkäyksen tarkoituksena on saada vastaus muodossa SYN/ACK. IP-paketin pienestä koosta johtuen, paketin ei pitäisi olla fragmentoitunut, joten fragmentoitunutta SYN-pakettia pidetään epäilyttävänä. Tästä syystä Junos käyttöjärjestelmän Screen *syn-frag* tarkistaa onko paketti fragmentoitunut sekä onko paketissa kohta SYN asetettuna. Mikäli näin on, paketti pudotetaan. (Juniper Networks Security Configuration Guide 2011, 943 - 944.)

5.4 Palvelunestohyökkäys (DoS Attack)

5.4.1 Yleistä

Palvelunestohyökkäyksen tarkoituksena on tukkia kohteen verkkoliikenne turhalla liikenteellä, jotta oikea liikenne ei pääse liikkumaan laitteistoissa. Kohde voi olla esimerkiksi palomuuri tai ihan yksittäinen käyttäjä. Jos palvelunestohyökkäys (DoS) saa alkunsa useasta lähde-osoitteesta, on sen nimi hajautettu palvelunestohyökkäys (DDoS). Palvelunestohyökkäykset on luokiteltu sen mukaan, mihin kohteeseen hyökkäys on tarkoitettu. (Juniper Networks Security Configuration Guide 2011, 947.)

5.4.2 Palomuuriin kohdistuva palvelunestohyökkäys

On mahdollista, että palvelunestohyökkäys kohdistetaan Juniper Networksin palomuuriin, jotta se ei pystyisi normaaliin toimintaan. Hyökkääjän tarkoituksena on tukkia istuntotaulu, joka pitää kirjaa olemassa olevista istunnoista. Kun istuntotaulu on tukittuna, ei palomuuri pysty enää muodostamaan uusia istuntoja ja liikenne tukkiutuu. Junos käyttöjärjestelmän Screeneillä on mahdollista rajata istuntojen määrää niin lähde-, kuin kohde osoitteistakin. Rajaamalla samasta IP-osoitteesta tulevia istuntopyyntöjä, vältetään istuntotaulukon ylikuormittuminen ja täten palvelunestohyökkäys. (Juniper Networks Security Configuration Guide 2011, 948.)

5.4.3 Verkon laitteisiin kohdistuva palvelunestohyökkäys

Palvelunestohyökkäyksen kohteena voi olla yksi tai useampi verkon laite. Tarkoituksena on tukkia laite suurella määrällä SYN, ICMP tai UDP -paketteja, jolloin kyseinen laite ei enää pysty välittämään paketteja eteenpäin. Kohteena voi olla yksittäinen tietokone tai verkon kriittinen reititin, jonka toimimattomuuden seurauksena koko verkon toiminta on vaarassa. (Juniper Networks Security Configuration Guide 2011, 955.)

5.4.4 Käyttöjärjestelmäkohtaiset palvelunestohyökkäykset

Jos hyökkääjä on saanut IP-osoitteiden ja porttien lisäksi tietoonsa kohteen käyttöjärjestelmän, on hyökkääjän mahdollista tehdä vielä tehokkaampia ja helposti toteutettavia hyökkäyksiä. Junos käyttöjärjestelmällä nämä hyökkäykset on mahdollista havaita ja estää, ennen kuin ne edes saapuvat kohteeseen. (Juniper Networks Security Configuration Guide 2011, 975.)

6 IPSec VPN

6.1 Virtual Private Network (VPN)

6.1.1 Yleistä

VPN-yhteys mahdollistaa kahden eri osapuolen turvallisen yhteyden Internetin yli. VPN-yhteys on mahdollista toteuttaa kahden verkon välille (site-to-site VPN) tai käyttäjän ja verkon välille. Liikenne näiden osapuolien välillä kulkee IP Security (IPSec) tunnelin välityksellä. IPSec on ryhmä TCP/IP protokollia, joilla turvataan liikenne Internetin yli. IPSec siis hoitaa liikenteen salauksen sekä osapuolten autentikoinnin. (Juniper Networks Security Configuration Guide 2011, 431.)

6.1.2 Turva-assosiaatio

Turva-assosiaatio (Security association, SA) on yksipuolinen sopimus VPN-yhteyden osapuolien välillä, jossa sovitaan yhteyden salauksen tyyppi ja autentikointi. Molemminpuolinen kommunikointi VPN-yhteyden avulla vaatii vähintään kaksi SA:ta, yksi molempiin suuntiin. SA:n avulla IPSec tunneli voi tarjota seuraavat ominaisuudet tietoturvan takaamiseksi:

- Yksityisyyden
- Tiedonsiirron eheyden
- Lähettäjän autentikoinnin

(Juniper Networks Security Configuration Guide 2011, 434.)

6.1.3 IPSec avainten hallinta

IPSec tunnelin osapuolten varmistaminen tapahtuu avainten avulla. Junos käyttöjärjestelmässä on mahdollista vaihtaa avaimet osapuolten kesken kolmella eri tavalla.

Manuaalisesti (Manual key)

Manuaalinen avaintenvaihto on yksinkertainen. Yhteyden molemmissa päissä pitää olla tiedossa sama salasana ja kaikki SA:n ominaisuudet on konfiguroitava erikseen. Tämä on hyvä tapa avaintenvaihdolle pienissä yrityksissä, jossa avainten hallinta on helppoa. (Juniper Networks Security Configuration Guide 2011, 435.)

Automaattisesti (AutoKey IKE)

Jos on tarve hallinnoida useampia tunneleita, tarvitaan avaintenvaihtotapa, jossa kaikkea ei tarvitse säätää manuaalisesti. IPSec käyttää tähän tarkoitukseen Internet Key Exchange (IKE) protokollaa. Junos käyttöjärjestelmässä tämä on mahdollista toteuttaa valmiiksi jaetuilla avaimilla tai sertifikaateilla. (Juniper Networks Security Configuration Guide 2011, 436.)

AutoKey IKE:n käyttäminen valmiiksi jaetuilla avaimilla toteutetaan aluksi samalla tavalla kuin manuaalinen avaintenvaihto. Molemmat osapuolet määrittelevät SA:n ominaisuudet ja molemmilla pitää olla tiedossa avain, jolla yhteys varmennetaan. Erona manuaaliseen avaintenvaihtoon on se, että tässä tapauksessa myöhemmin, kun avaimet pitäisi vaihtaa uudestaan, tapahtuu se käyttäen IKE protokollaa, joten avaintenvaihto onnistuu paljon helpommin kuin manuaalisessa avaintenvaihdossa. (Juniper Networks Security Configuration Guide 2011, 436.)

AutoKey IKE:n käyttäminen sertifikaateilla toteutuu siten, että molemmat osapuolet hankkivat sertifikaatin kohteelta, joka hallinnoi digitaalisia serfitikaatteja. Serfitikaatin jakajan pitää olla luotettu molemmille osapuolille. (Juniper Networks Security Configuration Guide 2011, 436.)

Diffie-Hellman (DH) avaintenvaihto algoritmi

Diffie-Hellman avaintenvaihtoalgoritmin avulla osapuolet pystyvät luomaan jaetun salaisen arvon, jolla yhteys varmennetaan. Tekniikan vahvuus piilee siinä, että salaisen arvon luonti onnistuu turvattoman verkon ylitse siten, että itse salaista arvoa ei missään vaiheessa siirretä turvattoman verkon yli. On olemassa viisi DH ryhmää, joista Junos käyttöjärjestelmä tukee ryhmiä 1,2,5 ja 14. Mitä suurempi ryhmän numero, sitä tehokkaampi ja enemmän aikaa vaativampi kyseinen salaus on. (Juniper Networks Security Configuration Guide 2011, 436.)

6.1.4 IPSec protokollat

IPSec käyttää kahta protokollaa, jolla tiedonsiirto turvataan. Nämä ovat nimeltään Authentication Header (AH) protokolla sekä Encapsulating Security Payload (ESP) protokolla. AH protokollalla pystytään tarkistamaan paketin autenttisuus, sisällön koskemattomuus ja paketin alkuperä. Autentikointi tapahtuu tarkistussummalla, joka

lasketaan Hash Message Authentication Code:n (HMAC) avulla käyttäen salaista avainta ja joko MD5 tai SHA-1 algoritmia. MD5 (Message Digest 5) algoritmilla luodaan 128-bittinen digitaalinen allekirjoitus, jolla varmistetaan sisältö ja lähteen autenttisuus. SHA-1 (Secure Hash Algorithm) algoritmilla luodaan 160-bittinen digitaalinen allekirjoitus. SHA-1 algoritmia pidetään tietoturvallisempana vaihtoehtona, koska se tekee digitaalisista allekirjoituksista pidempiä ja täten turvallisempia. (Juniper Networks Security Configuration Guide 2011, 437.)

ESP protokollalla voidaan turvata yksityisyys koodaamalla koko paketti salakielellä, autentikoida lähde ja varmistaa paketin sisällön oikeellisuus. ESP kapseloi koko IP otsikkokentän (otsikkokentän ja hyötykuorman) ja sen jälkeen liittää uuden IP otsikkokentän jo salattuun pakettiin. Tämä uusi IP otsikkokenttä sisältää kohteen osoitteen, jolla suojattu data pääsee läpi verkon. Autentikointi tapahtuu samoilla protokollilla, kuin AH protokollassa (MD5 tai SHA-1). ESP käyttää kolmea eri salakieltä, jolla tiedonsiirto voidaan koodata:

- Data Encryption Standard (DES) on lohkosalaus, joka suojaa liikenteen 56-bittisellä avaimella.
- Triple DES (3DES) on DES:stä vahvempi salaus (168-bittinen avain).
- Advanced Encryption Standard (AES) on uusi standardi, joka tarjoaa laajempaa yhteensopivuutta muiden laitteistojen kanssa. Junos käyttöjärjestelmä tukee AES:ia, joka luo 128-, 192- sekä 256-bittisiä avaimia.

(Juniper Networks Security Configuration Guide 2011, 437 – 438.)

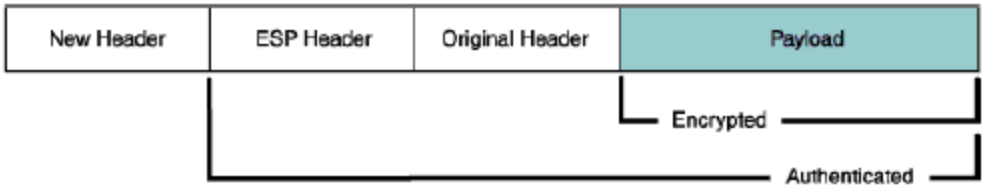
6.2 Tiedonsiirto IPSec-tunnelin välityksellä

6.2.1 Yleistä

IPSec VPN -tunneli sisältää tunnelin asetukset sekä tietoturvan. Tunnelia muodostettaessa, osapuolet muodostavat SA:t, jotka sisältävät tiedonsiirron turvaamiseen liittyvät parametrit. Kun tunneli on muodostettu, IPSec suojaa lähetetyn liikenteen aikaisemmin määriteltyjen SA:n mukaisesti

6.2.2 Pakettien prosessointi tunneli muodossa

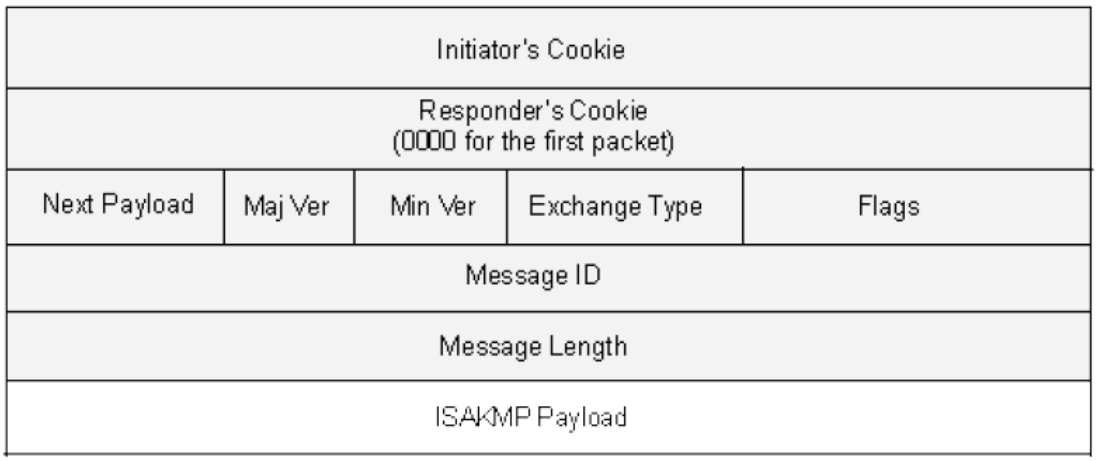
Yleisesti IPSec toimii joko kuljetus (transport mode) tai tunneli (tunnel mode) muodossa. Juniper Networksin laitteissa IPSec-pakettien prosessointi toimii aina tunneli muodossa. Tämä toimii siten, että koko IP-otsikkokenttä (hyötykuorma ja otsikkokenttä) kapseloidaan toiseen IP hyötykuormaan ja uusi otsikkokenttä liitetään siihen (ks. kuvio 20). (Juniper Networks Security Configuration Guide 2011, 440.)



KUVIO 20. Paketin prosessointi IPSec tunnelissa käyttäen ESP -protokollaa.
(Juniper Networks Security Configuration Guide 2011, 440)

6.2.3 IKE paketin prosessointi

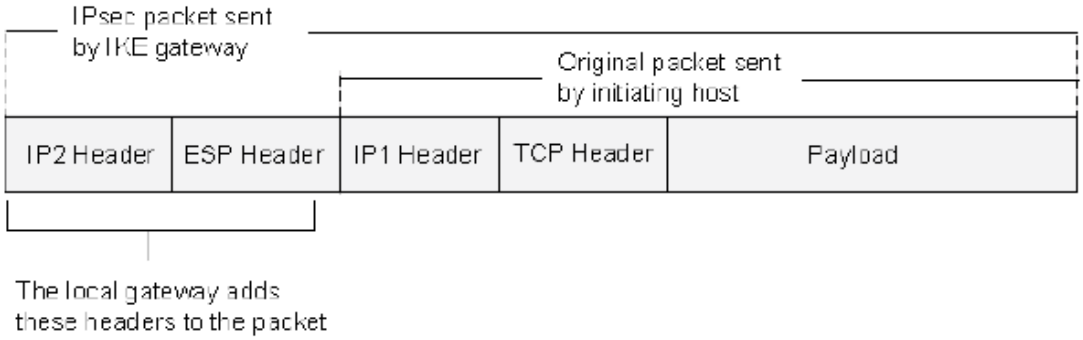
Kun tunnelointia vaativa selkokielinen paketti saapuu Juniper Networksin laitteelle ja aktiivista vaiheen kaksi SA:ta ei ole tälle tunnelille, Junos käyttöjärjestelmä aloittaa avaimen avaimenvaihto (Internet Key Excange) neuvottelun ja pudottaa paketin. Kun lähde lähettää pudotetun paketin uudestaan, on IKE neuvottelut käyty ja Junos käyttöjärjestelmä suojaa paketin ja kaikki tulevan istunnon paketit IPSec:llä, ennen kuin lähettää paketin eteenpäin. Kuviosta 21 selviää ISAKMP, eli IKE, -paketin muoto vaiheissa yksi ja kaksi. (Juniper Networks Security Configuration Guide 2011, 442.)



KUVIO 21. ISAKMP-paketti
(Juniper Networks Security Configuration Guide 2011, 442)

6.2.4 IPSec -paketin prosessointi

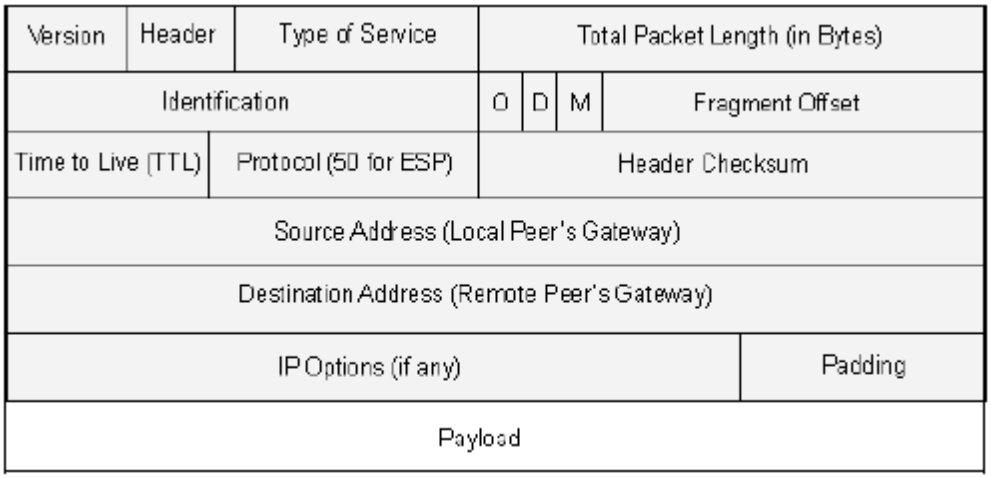
Kun IKE neuvottelut on saatu valmiiksi ja kaksi IKE yhdyskäytävää ovat muodostaneet vaiheen yksi ja kaksi SA:t, lähetetään liikenne eteenpäin tunnelia pitkin. Kuviossa 22 on IPSec-paketti käyttäen ESP-protokollaa. (Juniper Networks Security Configuration Guide 2011, 444.)



KUVIO 22. IPSec paketti käyttäen ESP -protokollaa

(Juniper Networks Security Configuration Guide 2011, 445)

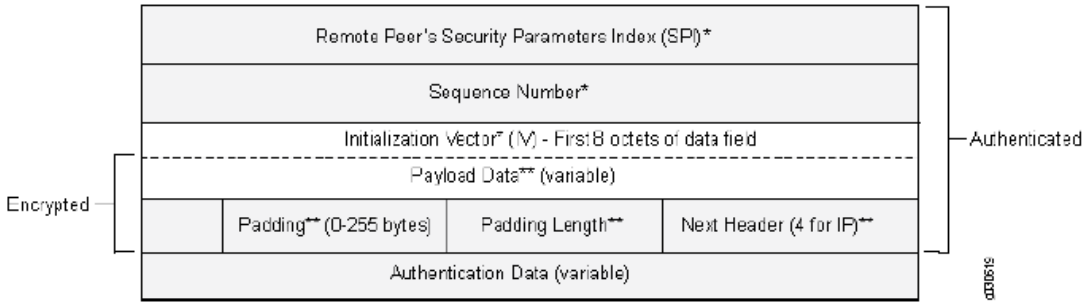
IP2 Header on Junos käyttöjärjestelmän lisäämä otsikkokenttä, joka sisältää etäyhdyskäytävän osoitteen (kohdeosoite) ja paikallisen reitittimen osoitteen (lähdeosoite). IP2 otsikkokenttä kuviossa 23.



KUVIO 23. IP2 otsikkokenttä

(Juniper Networks Security Configuration Guide 2011, 445)

ESP otsikkokenttä sisältää kohteen tarvitsemia tietoja paketin oikeanlaisesta prosessoinnista. Kuviossa 24 on ESP otsikkokenttä.



KUVIO 24. ESP otsikkokenttä

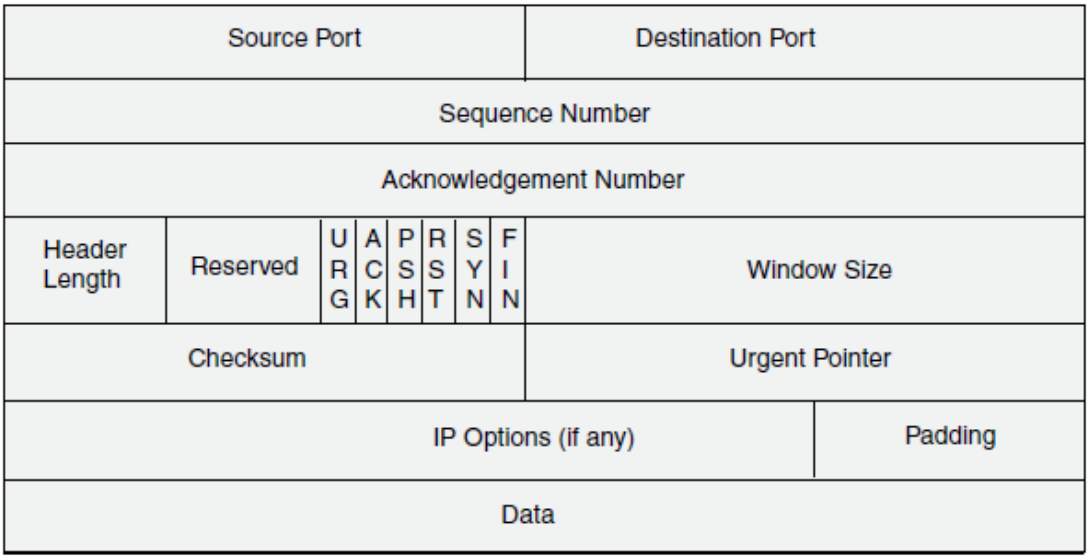
(Juniper Networks Security Configuration Guide 2011, 445)

IP2-otsikkokentän ja ESP-otsikkokentän jälkeen tulee sisempi IP-otsikkokenttä (IP1), jossa on lähde- ja kohdeosoitteet, jonka jälkeen tulee TCP (Transmission Control Protocol) -otsikkokenttä (ks. kuviot 25 ja 26).

Version	Header	Type of Service	Total Packet Length (in Bytes)			
Identification			O	D	M	Fragment Offset
Time to Live (TTL)	Protocol (6 for TCP)		Header Checksum			
Source Address (Installing Host)						
Destination Address (Receiving Host)						
IP Options (if any)						Padding
Payload						

KUVIO 25. IP1 otsikkokenttä

(Juniper Networks Security Configuration Guide 2011, 446)



KUVIO 26. TCP otsikkokenttä

(Juniper Networks Security Configuration Guide 2011, 446)

6.3 IKE tunneli

6.3.1 Tunnelin muodostaminen

Ensimmäisessä vaiheessa IKE tunnelin luontia vaihdetaan ehdotuksia (proposal) siitä, kuinka autentikoidaan ja turvataan yhteys. Osapuolet vaihtavat ehdotuksia hyväksyttävistä tietoturvaominaisuuksista, kuten:

- Liikenteen salaus algoritmit (DES, 3DES ja AES)
- Autentikointi algoritmit (MD5 ja SHA-1)
- Diffie-Hellman algoritmin ryhmä
- AutoKey IKE (ennaltamääritetyillä avaimilla vai sertifikaateilla)

Onnistunut vaiheen yksi neuvottelu loppuu silloin, kun molemmat osapuolet sopivat ainakin yhden ehdotuksen turvaparametreihin ja prosessoi niiden mukaan. Juniper Networksin laitteissa on mahdollista määritellä neljä ehdotusta, joka määrittelee sen kuinka tietoturvallinen avaintenjakoprosessi hyväksytään. Junos käyttöjärjestelmässä on ennalta määritettyjä vaiheen yksi ehdotuksia, mutta on myös mahdollista luoda uusia ehdotuksia. Vaihe yksi voi tapahtua joko yleisellä toimintatavalla (main mode) tai aggressiivisella toimintatavalla (aggressive mode). (Juniper Networks Security Configuration Guide 2011, 447)

6.3.2 Yleinen toimintatapa (Main mode)

Yleisessä toimintatavassa lähetetään yhteensä kuusi viestiä kolmessa kahdensuuntaisessa vaihdossa.

1. Ensimmäinen vaihto (viestit 1 ja 2) – Ehdotetaan ja hyväksytään koodaus ja autentikointi algoritmit.
2. Toinen vaihto (viestit 3 ja 4) – Suoritetaan Diffie-Hellman exchange ja molemmat osapuolet toimittavat satunnaisen numeron (DH:ta varten).
3. Kolmas vaihto (viestit 5 ja 6) – Lähetetään ja varmistetaan osapuolten identiteetti

Kolmannessa vaihdossa lähetetyt viestit suojataan koodausalgoritmilla, joka päätetään kahdessa ensimmäisessä vaihdossa. Tämän takia osapuolten identiteetit on salattu heti yhteyden luonnin alusta saakka. (Juniper Networks Security Configuration Guide 2011, 447 – 448.)

6.3.3 Aggressiivinen toimintatapa (Aggressive Mode)

Aggressiivisessa toimintatavassa osapuolet toteuttavat samat asiat kuin yleisessä toimintatavassa, mutta vain kahdella vaihdolla ja yhteensä kolmella viestillä.

1. Ensimmäinen viesti – Yhteyden aloittaja ehdottaa SA:ta, ehdottaa DH:ta ja lähettää satunnaisen numeron (DH:ta varten) ja hänen IKE identiteetin.
2. Toinen viesti – Yhteyden vastaanottaja hyväksyy SA:n autentikoi yhteyden aloittajan ja lähettää satunnaisen numeron (DH:ta varten), hänen IKE identiteetin ja sertifikaatin (jos sertifikaatit käytössä).
3. Kolmas viesti – Yhteyden aloittaja autentikoi vastaanottajan, hyväksyy DH:n ja lähettää oman sertifikaatin (jos käytössä).

Koska ensimmäisessä kahdessa viestissä osapuolten identiteetit vaihdetaan suojaamattomasti, aggressiivinen toimintatapa ei turvaa identiteettiä. (Juniper Networks Security Configuration Guide 2011, 448.)

6.4 IPSec-tunneli

Kun osapuolet ovat muodostaneet turvallisen ja autentikoidun kanavan vaiheessa yksi, suorittavat ne vaiheen kaksi. Vaiheessa kaksi neuvotellaan SA:t joiden mukaan tieto kuljetetaan IPSec tunnelin läpi. Kuten vaiheessa yksi, osapuolet vaihtavat ehdotuksia, millä määritellään turvaparametrit, jotka sidotaan SA:han. Vaihe kaksi sisältää koodauksen ja autentikoinnin lisäksi IPSec protokollan (ESP tai AH). Ehdotus voi myös määritellä DH-ryhmän, jos Perfect Forward Secrecy (PFS) halutaan aktivoida. PFS on

keino, jolla vaiheen kaksi avainten derivointi on erillinen ja riippumaton edellisistä avaimista. Tämä tapahtuu siten, että vaiheen yksi ehdotuksissa luodaan avain (SKEYID-d), josta kaikki vaiheen kaksi avaimet derivoidaan. Valitettavasti kaikki avaimet ovat vaarassa paljastua, jos SKEYID-d avain joutuu vääriin käsiin. Tämä riski huomioidaan PFS:ssä pakottamalla DH-avaimenvaihto jokaisen vaiheen kaksi tunnelin kohdalla. PFS:n käyttö on siis turvallisempaa, mutta se voi hidastaa prosessia. (Juniper Networks Security Configuration Guide 2011, 449 – 450.)

Vaiheessa kaksi käytetään vain nopeata tyyliä (quick mode). Nopea tyyli sisältää kolme viestiä. Myös vaiheessa kaksi on ennalta määriteltyjä ehdotuksia, mutta myös uusien ehdotusten luominen on mahdollista. (Juniper Networks Security Configuration Guide 2011, 449 – 450.)

6.5 Reittipohjainen VPN-yhteys (Route-based VPN)

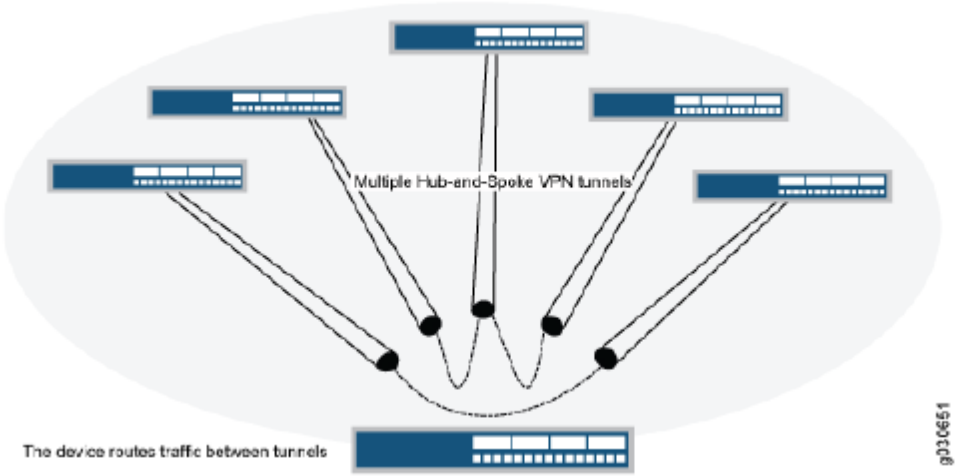
Reittipohjaiseen VPN-yhteyteen voidaan konfiguroida monia turvasääntöjä (security policy), joilla liikennettä rajataan. Liikenne kulkee yhden VPN-tunnelin läpi, jossa on vain yhdet SA:t toiminnassa. Reittipohjaisessa VPN-yhteydessä turvasääntö viittaa kohdeosoitteeseen eikä VPN-tunneliin. Kun Junos käyttöjärjestelmä selvittää reittiä löytääkseen rajapinnan, jonka kautta liikenne pääsee kohteeseen, löytää se reitin turvatun tunnelin rajapinnan kautta. Tunnelin rajapinta on sidoksissa määriteltyyn VPN-tunneliin, jota pitkin liikenne kulkee, mikäli turvasäännöt sen sallii. (Juniper Networks Security Configuration Guide 2011, 433.)

6.6 Sääntöpohjainen VPN-yhteys (Policy-based VPN)

Sääntöpohjaisessa VPN-yhteydessä turvasääntö määrittelee, mikäli VPN-tunnelia käytetään. Säännössä viitataan VPN:n nimeltä, mikäli liikenteelle sallitaan VPN-tunnelin käyttö. Sääntöpohjaisessa VPN:ssä jokainen sääntö luo yksilöllisen IPSec SA:n, jonka katsotaan olevan yksilöllinen VPN-tunneli. Koska jokaiselle säännölle luodaan oma VPN-tunneli, vaatii sääntöpohjainen VPN-yhteys enemmän resursseja kuin reittipohjainen VPN-yhteys. (Juniper Networks Security Configuration Guide 2011, 432.)

6.7 Verkostomallinen VPN-yhteys (Hub and spoke VPN)

Verkostomallinen VPN-yhteys tarkoittaa sitä, että yhteen laitteeseen luodaan VPN-yhteyksiä monesta eri laitteesta ja halutaan, että nämä etälaitteet pystyvät kommunikoimaan myös keskenään tietoturvallisesti. Jotta tämä on mahdollista, on myös turvasääntöjä luotava tunneleiden välille. Kuviossa 27 on verkostomallinen VPN-yhteys. (Juniper Networks Security Configuration Guide 2011, 485 – 486.)



KUVIO 27. Verkostomallinen VPN-yhteys

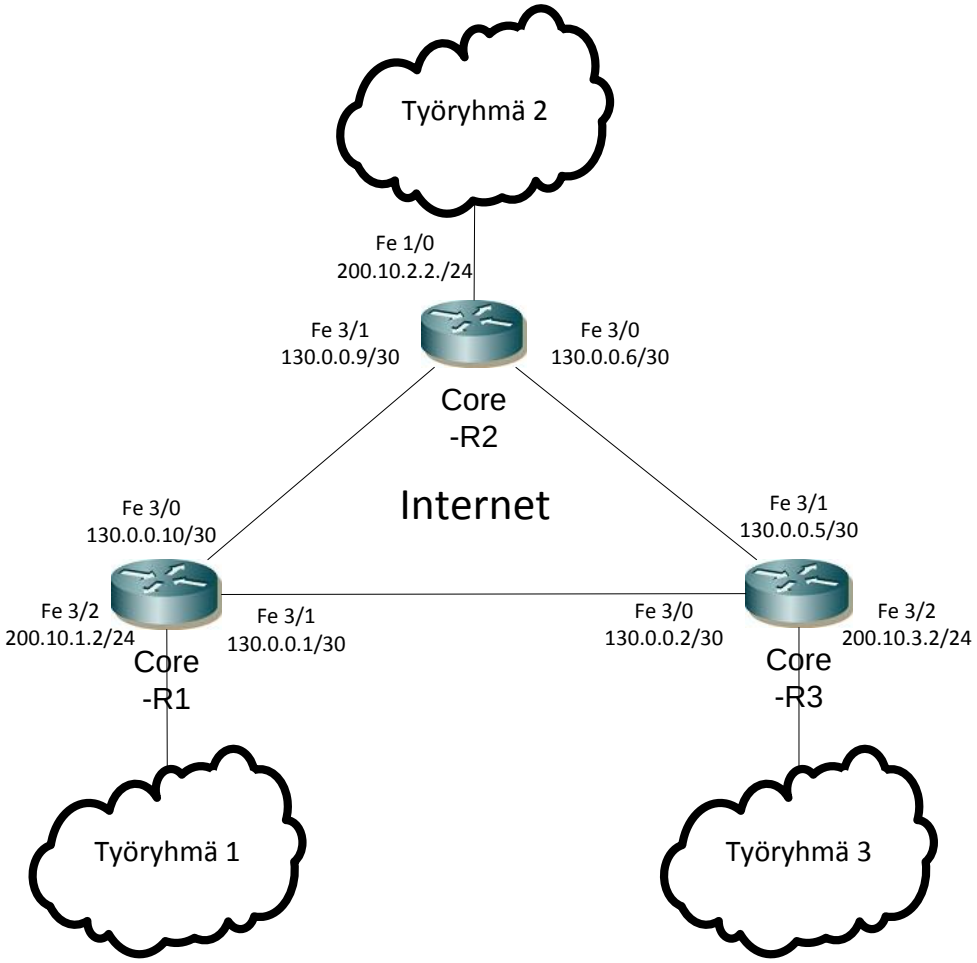
(Juniper Networks Security Configuration Guide 2011, 486)

7 Käytännön toteutus

7.1 Laitteisto ja topologia

7.1.1 Internet

Internetin simuloimiseen käytettiin kolmea SpiderNetistä löytyvää Cisco Core -reititintä. Tässä työssä Internetin oli tarkoitus olla yksinkertainen. Kuviosta 28 selviää Internetin topologia ja liitännät yrityksen verkkoihin. Taulukossa 1 on lista IP-osoitteista ja käytetyistä rajapinnoista.



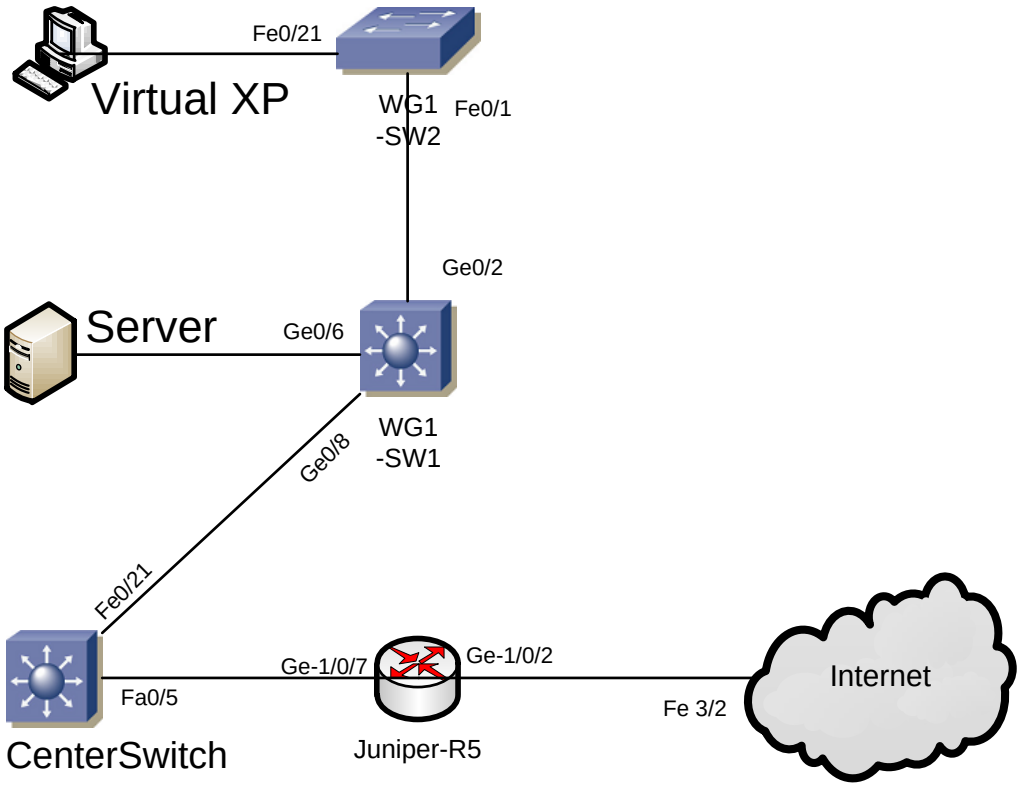
KUVIO 28. Internetin topologia

Taulukko 1. "Internetin" laitteiden IP-osoitteet ja portit

Laite	Rajapinta	IP-osoite	Kohdelaite	Kohteen rajapinta	IP-osoite
CiscoCore-R1	Fe 3/0	130.0.0.10/30	CiscoCore-R2	Fe 3/1	130.0.0.2/30
CiscoCore-R1	Fe 3/1	130.0.0.1/30	CiscoCore-R3	Fe 3/0	130.0.0.9/30
CiscoCore-R1	Fe 3/2	200.10.1.2/24	Juniper-R5	Ge 1/0/2	200.10.1.1/24
CiscoCore-R1	Loopback 0	130.0.3.1/30			
CiscoCore-R2	Fe 3/0	130.0.0.6/30	CiscoCore-R1	Fe 3/1	130.0.0.5/30
CiscoCore-R2	Fe 3/1	130.0.0.9/30	CiscoCore-R3	Fe 3/0	130.0.0.10/30
CiscoCore-R2	Fe 1/0	200.10.2.2/24	WG2-R1	Ge 0/0	200.10.2.1/30
CiscoCore-R2	Loopback 0	130.0.5.1/30			
CiscoCore-R3	Fe 3/0	130.0.0.2/30	CiscoCore-R1	Fe 3/1	130.0.0.1/30
CiscoCore-R3	Fe 3/1	130.0.0.5/30	CiscoCore-R2	Fe 3/0	130.0.0.6/30
CiscoCore-R3	Fe 3/2	200.10.3.2/24	Juniper-R4	Ge 1/0/2	200.10.3.1/24
CiscoCore-R3	Loopback 0	130.0.4.1/30			

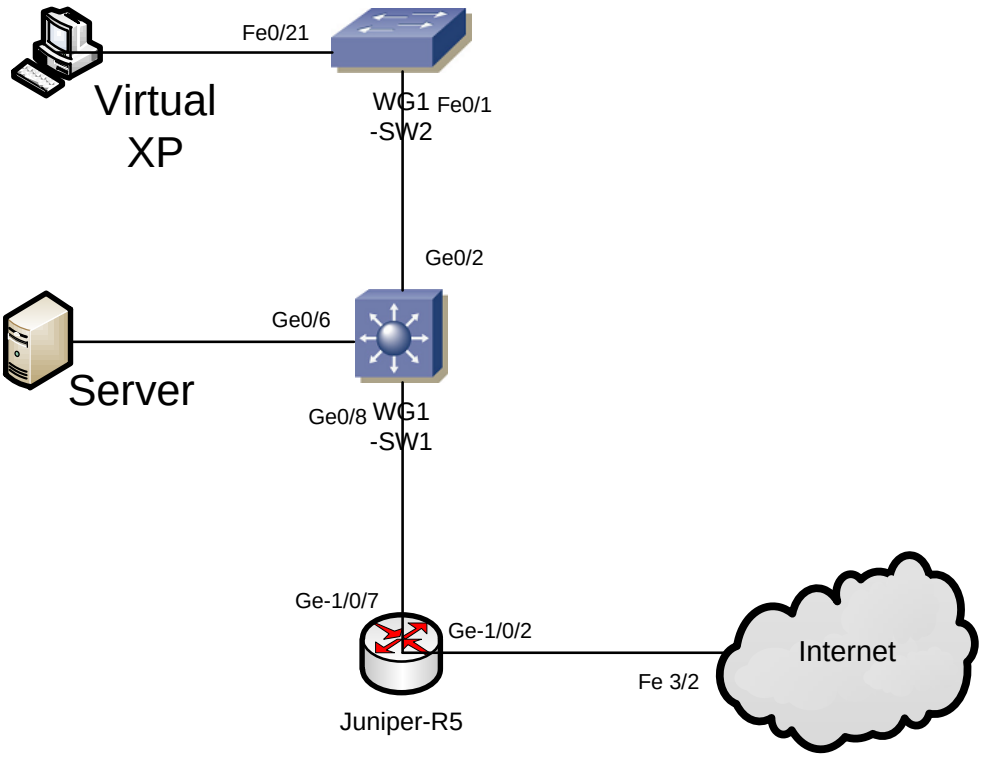
7.1.2 Yrityksen työryhmät

Yrityksen työryhmä ja työryhmä 3 koostuvat kahdesta Cisco Systemsin kytkimestä sekä yhdestä Juniper Networksin J-series reitittimestä. Jäljelle jäävä työryhmä 2 on muuten samanlainen, mutta Juniper Networksin J-series reitittimen sijaan siinä on Cisco Systemsin reititin. Kuviossa 29 on esitettynä työryhmän yksi topologia. Tässä on mukana keskuskytkin, joka vain siis välittää VLAN tiedolla varustetut tiedot WG1-SW1:ltä Juniper-R5:lle.

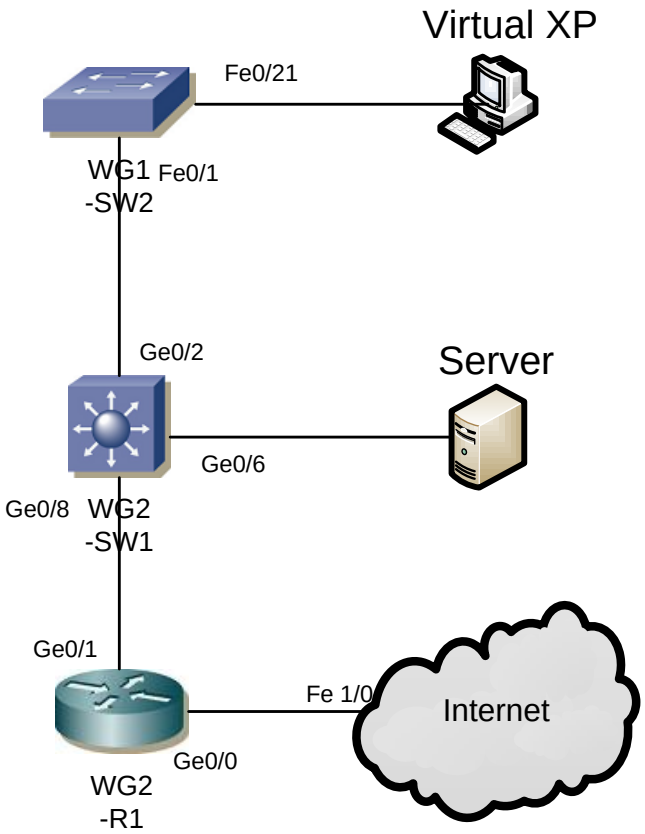


KUVIO 29. Työryhmän yksi topologia. Mukana myös keskuskytkin.

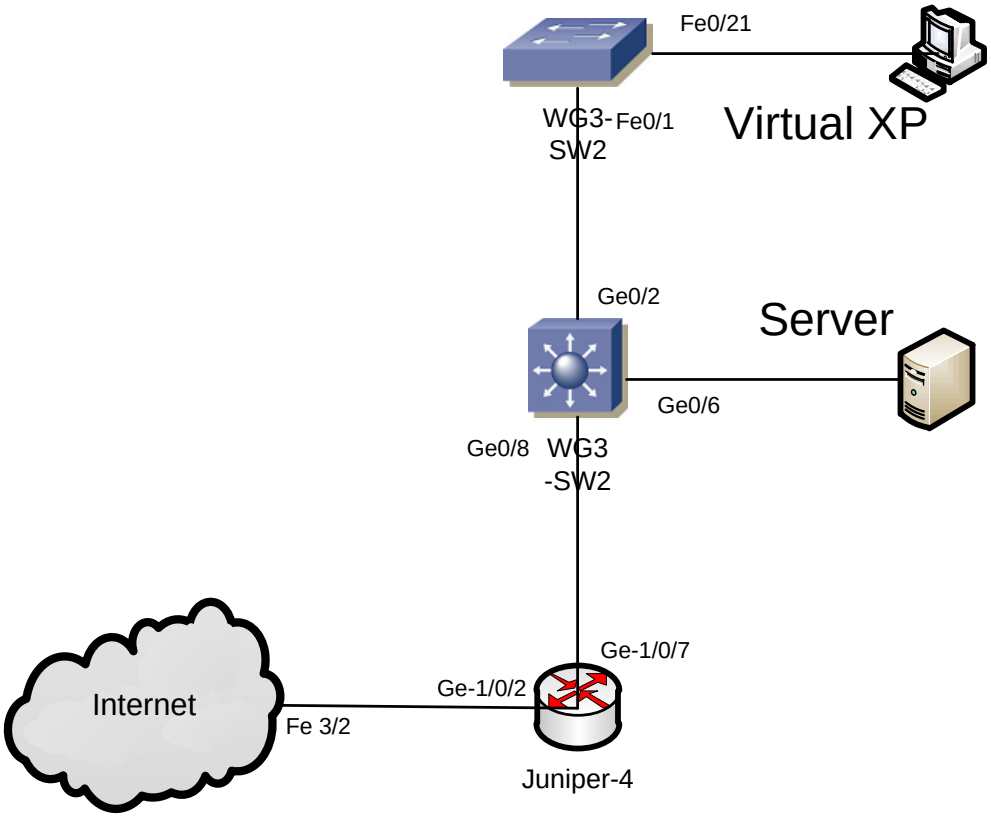
Työ tehtiin siten, että kyseistä keskuskytkintä ei huomioitu topologiassa. Keskuskytkin on todellisuudessa mukana myös työryhmän kaksi topologiassa, mutta sitäkään ei työssä huomioida. Työryhmien topologiat ilman keskuskytkintä näyttävät kuvioiden 30, 31 ja 32 mukaisilta.



KUVIO 30. Työryhmän yksi topologia.



KUVIO 31. Työryhmän kaksi topologia



KUVIO 32. Työryhmän kolme topologia.

Seuraavista taulukoista 2,3 ja 4 selviää työryhmissä käytetyt IP-osoitteet ja rajapinnat.

Taulukko 2. Työryhmän yksi IP-osoitteet ja rajapinnat

Laite	Rajapinta	IP-osoite
Juniper-R5	ge-1/0/2.0	200.10.1.1/24
Juniper-R5	ge-1/0/7.10	192.168.1.1/25
Juniper-R5	ge-1/0/7.20	192.168.1.129/25
Juniper-R5	loopback0	172.16.4.1/32
WG1-SW1	VLAN 10	192.168.1.1/25
WG1-SW1-server	Ge 0/6	192.168.1.10/25
WG1-SW2	VLAN 20	192.168.1.129.25
WG1-SW2-XP	Fe 0/21	192.168.1.130/25

Taulukko 3. Työryhmän kaksi IP-osoitteet ja rajapinnat

WG2-R1	ge0/0	200.10.2.1/24
WG2-R1	ge0/1.30	192.168.1.1/25
WG2-R1	ge0/1.40	192.168.2.129/25
WG2-R1	loopback0	172.16.5.1/32
WG1-SW1	VLAN 30	192.168.1.1/25
WG1-SW1-server	Ge 0/6	192.168.1.10/25
WG1-SW2	VLAN 40	192.168.1.129.25
WG1-SW2-XP	Fe 0/21	192.168.1.130/25

Taulukko 4. Työryhmän kolme IP-osoitteet ja rajapinnat

Juniper-R4	ge-1/0/2.0	200.10.3.1/24
Juniper-R4	ge-1/0/7.50	192.168.3.1/25
Juniper-R4	ge-1/0/7.60	192.168.3.129/25
Juniper-R4	loopback0	172.16.6.1/32
WG1-SW1	VLAN 50	192.168.3.1/25
WG1-SW1-server	Ge 0/6	192.168.3.10/25
WG1-SW2	VLAN 60	192.168.3.129/25
WG1-SW2-XP	Fe 0/21	192.168.1.130/25

7.2 Internetin konfigurointi

Internetin konfigurointi pidettiin mahdollisimman yksinkertaisena. Reititysprotokollaksi valittiin Open Shortest Path First (OSPF) -protokolla. Konfigurointi helppo toteuttaa, koska ”Internetin” simulointiin käytettiin vain kolmea CiscoCore-reititintä. OSPF vaatii toimiakseen reitittimen ID:n (Router ID), jonka se ottaa tässä tapauksessa Loopback 0 -rajapinnalta. Yhteys ”Internetistä” yrityksen verkkoihin konfiguroitiin staattisen reitin avulla.

Esimerkkinä CiscoCore-R1 konfiguraatiot:

```
interface Loopback0
 ip address 130.0.3.1 255.255.255.252
!
interface FastEthernet3/0
 description "Link to CiscoCore-R2"
 no switchport
 ip address 130.0.0.10 255.255.255.252
!
interface FastEthernet3/1
```

```
 description "Link to CiscoCore-R3"
 no switchport
 ip address 130.0.0.1 255.255.255.252
!
interface FastEthernet3/2
 description "Link to Juniper-R5"
 no switchport
 ip address 200.10.1.2 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 network 130.0.0.0 0.0.0.3 area 0
 network 130.0.0.8 0.0.0.3 area 0
 network 130.0.3.0 0.0.0.3 area 0
 network 200.10.1.0 0.0.3 area 0
!
```

Yläpuolella olevassa konfiguraatiossa määriteltiin ensin IP-osoitteet ja aliverkon peitteet tarvittaville rajapinnoille, jonka jälkeen konfiguroitiin OSPF. Lopuksi määritellään vielä staattinen reitti työryhmän yksi reitittimelle Juniper-R5. Kaikki CiscoCore -reitittimien konfiguraatiot ovat liitteissä 10-12.

7.3 Työryhmien konfigurointi

Työryhmissä on yksi reititin ja kaksi kytkintä. Nämä kaksi kytkintä (WGx-SW1 ja WGx-SW2) on kaikissa työryhmissä konfiguroitu samalla tavalla jokaisen työryhmän omilla IP-osoitteilla. Esimerkkinä osa WG1-SW2 konfiguraatiosta:

```
!
vlan 10
 name Palvelin
!
vlan 20
 name Tyoasema
!
interface FastEthernet0/1
 description Link to wg1-sw1
 switchport mode trunk
!
!
interface range FastEthernet0/2 - 12
 switchport access vlan 10
 switchport mode access
 shutdown
!
interface FastEthernet0/21
 description Virtual XP
```

```
 switchport access vlan 20
 switchport mode access
 speed 100
!
```

Aluksi määriteltiin VLAN:t, jonka jälkeen konfiguroitiin rajapinnat. Rajapinta FastEthernet 0/1 määriteltiin trunk-tilaan, jotta yhteys kahden kytkimen välille saatiin muodostettua. Rajapinnat FastEthernet 0/2 – 0/24 määriteltiin access-tilaan kahdella eri VLAN leimalla (10 ja 20). Rajapinnassa FastEthernet 0/21 on kiinni virtuaalinen XP-Vmware työasema.

Työryhmän kytkimen WGx-SW1:sen konfiguraatiot ovat myös hyvin yksinkertaiset. Aluksi määritellään samat VLAN:t kuin WG1-SW2:sessakin, jonka jälkeen määritellään rajapinnat. Alapuolella osa WG1-SW1:sen konfiguraatioista:

```
vlan 10
 name Palvelin
!
vlan 20
 name Tyoasema
!
interface GigabitEthernet0/2
 description "Trunk to WG1-SW2"
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 speed 100
!
interface GigabitEthernet0/6
 description "Server"
 switchport access vlan 10
 switchport mode access
 speed 100
!
interface GigabitEthernet0/8
 description "Link to Centerswitch --> Juniper-R5"
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
```

Yhteys WG1-SW2:seen tapahtuu rajapinnan GigabitEthernet 0/2 kautta, joka asetettiin trunk tilaan. Rajapinta GigabitEthernet 0/6 yhdistää työssä käytettävän palvelimen kytkimeen WG1-SW1. Yhteys laitteiden WG1-SW1 ja Juniper-R5 välille jouduttiin SpiderNetin topologian takia muodostamaan ns. keskuskytkimen (Centerswitch) kaut-

ta, joka vain välittää tiedon eteenpäin. Yhteys keskuskytkimeen ja sitä kautta Juniper-R5 -reitittimelle tapahtuu rajapinnan *GigabitEthernet 0/8* kautta käyttämällä VLAN leimoja 10 ja 20.

Jotta yhteys Juniper-R5-reitittimen kautta Internetiin saatiin toimimaan, oli laitteelle konfiguroitava normaalisti rajapinnat, staattinen reitti, turva-alueet (security zone) ja turvasäännöt (security policy). Turva-alueiden ja -sääntöjen konfiguroiminen käydään läpi kappaleessa 7.4. Esimerkkinä Juniper-R5 reitittimen peruskonfiguraatiot:

```
interfaces {
   ge-1/0/2 {
      unit 0 {
         family inet {
            address 200.10.1.1/24;
         }
      }
   }
   ge-1/0/7 {
      vlan-tagging;
      unit 10 {
         vlan-id 10;
         family inet {
            address 192.168.1.1/25;
         }
      }
      unit 20 {
         vlan-id 20;
         family inet {
            address 192.168.1.129/25;
         }
      }
   }
   lo0 {
      unit 0 {
         family inet {
            address 172.16.4.1/32;
      }
   }
}
routing-options {
   static {
      route 0.0.0.0/0 next-hop 200.10.1.2;
 }
   router-id 172.168.4.1;
}
}
```

Aluksi määriteltiin yhteydellisyys välille WG1-SW1 ja Juniper R5. Tämä tapahtui konfiguroimalla rajapinta Ge-1/0/7 käyttämään VLAN-leimoja (VLAN-tagging) ja määriteltiin VLAN-leimat sekä tarvittavat IP-osoitteet. Reititys Internetiin tehtiin staattisesti rajapinnan Ge-1/0/2 kautta.

Seuraavaksi tärkeimmät kohdat WG2-R1:sen konfiguroinnista:

```
interface GigabitEthernet0/0
 ip address 200.10.2.1 255.255.255.0
 duplex auto
 speed auto
!
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 no shutdown
!
interface GigabitEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.2.1 255.255.255.128
!
interface GigabitEthernet0/1.40
 encapsulation dot1Q 40
 ip address 192.168.2.129 255.255.255.128
!
ip route 0.0.0.0 0.0.0.0 200.10.2.1
```

WG2-R1 konfiguroitiin ensin rajapinnoille tarvittavat IP-osoitteet, aktivoitiin dot1Q kapselointi rajapinnoissa ge0/1.30 ja ge0/1.40. Lopuksi konfiguroitiin staattinen reitti CiscoCore-R2:lle.

7.4 Tietoturvaominaisuuksien konfigurointi

7.4.1 Turva-alueiden konfigurointi

Turva-alueiden konfiguroinnin esimerkkinä käytän turva-alueen wg1 konfiguraatiota:

```
security {
    security-zone wg1 {
        address-book {
            address wg1 192.168.1.128/25;
            address admin 192.168.1.130/32;
            }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-1/0/7.20;
        }
    }
}
```

Konfigurointi tapahtui seuraavasti:

```
root@Juniper-R5# set security zones security-zone wg1
root@Juniper-R5# edit security zones security-zone wg1
```

Konfiguroinnissa määriteltiin aluksi turva-alueen nimeksi wg1 ja siirryttiin editoimaan sitä.

```
[edit security zones security-zone wg1]
root@Juniper-R5# set address-book address wg1 192.168.1.128/25
root@Juniper-R5# set address-book address admin 192.168.1.130/32
root@Juniper-R5# set host-inbound-traffic system-services all
root@Juniper-R5# set host-inbound-traffic protocols all
root@Juniper-R5# set interfaces ge-1/0/7.20
```

Tämän jälkeen määriteltiin turva-alueen wg1 osoitekirjat ja niihin osoitteet, sallittiin protokollat ja palvelut sekä sidottiin rajapinta ge-1/0/7.20 turva-alueeseen. Loput turva-alueiden konfiguroinnit selviävät kunkin Juniper-reitittimen konfiguraatioista, jotka löytyvät liitteistä 1 ja 5.

7.4.2 Turvasääntöjen konfigurointi

Turvasääntöjen (Security policy) konfigurointi aloitetaan määrittelemällä turva-alueet, joita säännöt koskevat. Tässä tapauksessa tutkitaan turvasääntöjä, jotka koskevat turva-alueita wg1 ja server.

```
security {
    policies {
    from-zone server to-zone wg1 {
       policy salli {
          match {
             source-address any;
             destination-address any;
             application any;
          }
          then {
             permit;
          }
       }
    }
```

Yläpuolella esimerkki turvasäännöstä *salli*, jolla sallitaan kaikki liikenne turva-alueelta *server* turva-alueelle *wg1*. Konfigurointi:

```
root@Juniper-R5# set security policies from-zone server to-zone wg1 policy salli
root@Juniper-R5# edit security policies from-zone server to-zone wg1 policy salli
[edit security policies from-zone server to-zone wg1 policy salli]
root@Juniper-R5# set match source-address any
root@Juniper-R5# set match destination-address any
root@Juniper-R5# set match application any
root@Juniper-R5# set then permit
```

Aluksi luodaan turvasääntö nimeltä salli ja siirrytään *edit* -komennolla muokkaamaan turvasääntöä. Tämän jälkeen määritellään vastaavuus kriteereiksi kaikki osoitteet ja sovellukset, jonka jälkeen määritetään toiminto *permit*.

Aikaisemmassa esimerkissä sallittiin siis liikenne turva-alueelta server alueelle wg1. Jotta jotain liikennettä pääsisi liikkumaan myös toiseen suuntaan määriteltävä säännöt. Policyjä testatakseni, määrittelin yhden IP-osoitteen turva-alueen wg1 aliverkosta osoitekirjaan nimeltä admin. Tälle kyseiselle osoitekirjalle, eli IP-osoitteelle 192.168.1.130/25 annoin oikeudet ottaa telnet yhteyden palvelimelle. Alapuolella esimerkkinä konfiguraatiot säännöistä admin, deny-telnet ja permit.

```
from-zone wg1 to-zone server {
   policy admin {
      match {
         source-address admin;
         destination-address server;
         application any;
      }
      then {
         permit;
      }
   }
   policy deny_telnet {
      match {
         source-address any;
         destination-address any;
         application junos-telnet;
      }
      then {
         deny;
      }
   }
   }
   policy permit  {
      match {
         source-address any;
         destination-address any;
         application any;
      }
      then {
         permit;
      }
   }
```

Turvasääntöjen tulkitseminen tapahtuu järjestyksessä ylhäältä alaspäin, joten sijoitin admin osoitekirjaa koskevan säännön ensimmäiseksi, telnet ohjelman kieltävän säännön toiseksi ja kaiken sallivan säännön kolmanneksi. Demonstraatio turvasääntöjen toimivuudesta löytyy kappaleesta 8.2 Kaikki loput turvasääntöjen konfiguraatiot kokonaisuudessaan löytyvät liitteistä 1 ja 5.

7.4.3 Screenien konfigurointi

Screenien konfiguraatio Junos käyttöjärjestelmässä on yksinkertaista. Aluksi asetetaan Screenille nimi, johon sidotaan haluttavat Screen vaihtoehdot. Tämän jälkeen Screen on vielä sidottava haluttuun turva-alueeseen, jonka jälkeen Screen on aktivoitu.

Alapuolella esimerkki Screen:stä nimeltä testi, jolla estetään hyökkäykset ICMP large (ylisuuret ICMP-paketit), port-scan (porttiskannaus) ja SYN-FLOOD (SYN-pakettien tulvitus)

```
security {
   screen {
      ids-option testi {
         icmp {
            large;
         }
         tcp {
            port-scan threshold 5000;
            syn-flood;
}
}
}
}
```

Konfigurointi:

root@Juniper-R5# set security screen ids-option testi
root@Juniper-R5# edit security screen ids-option testi
[edit security screen ids-option testi]
root@Juniper-R5# set icmp large
root@Juniper-R5# set tcp port-scan threshold 5000
root@Juniper-R5# set tcp syn-flood

Tämän jälkeen kyseinen Screen pitää siis vielä aktivoida haluttuun turva-alueeseen:

root@Juniper-R5#set security zones security-zone server screen testi

Eri Screenien toimivuus todetaan kappaleessa 8.4.

7.4.4 NAT (Network Address Translation) konfigurointi

Tässä työssä konfiguroitiin kahdenlainen NAT, staattinen (Static) ja lähde (Source) NAT. Staattinen NAT konfiguroitiin yksi-yhteen osoitteen muutoksella työryhmän yksi palvelimelle ja lähde NAT konfiguroitiin työryhmän yksi aliverkolle 192.168.1.129/25 eli osoiteryhmä wg1:lle. Alapuolella esimerkki staattisen NAT:n konfiguraatiosta, laitteessa Juniper-R5:

set security nat static rule-set rs-static from zone internet
set security nat static rule-set rs-static rule r-static match destination-address 200.10.1.10/32
set security nat static rule-set rs-static rule r-static then static-nat prefix 192.168.1.10/32

Konfiguraatiossa määriteltiin aluksi sääntöryhmä (rule-set), johon liitetään tämän jälkeen säännöt (rule). Säännöksi konfiguraatiossa asetettiin turva-alueesta internet tulevien yhteyksien osoitteen muutoksen julkisesta osoitteesta 200.10.1.10/32, yksityiseen osoitteeseen 192.168.1.10/32.

set security nat proxy-arp interface ge-1/0/2.0 address 200.10.1.10/32

Lopuksi määriteltiin vielä rajapintaan ge-1/0/2.0 proxy-arp osoitteella 200.10.1.10/32, jotta rajapinta osasi käsitellä kyseisellä IP-osoitteella tulevat ARP -yhteyspyynnöt.

Kohde NAT (source NAT) muodostettiin yksityiselle aliverkolle 192.168.1.129/25. Tarkoituksena oli, että kyseinen aliverkko saisi julkiset osoitteet Internetiin päin menevälle liikenteelle. Seuraavana kohde NAT:n konfiguraatiot Juniper-R5:sta:

set security nat source pool pool1 address 200.10.1.129/32 to 200.10.1.142/32
set security nat source rule-set rs-source from zone wg1
set security nat source rule-set rs-source to zone internet
set security nat source rule-set rs-source rule r-source match source-address 192.168.1.129/25
set security nat source rule-set rs-source rule r-source match destination-address 0.0.0.0/0
set security nat source rule-set rs-source rule r-source then source-nat pool pool1

Aluksi konfiguroitiin lähdeosoitteille osoiteryhmä (source address pool), johon myöhemmin konfiguraatiossa viitataan. Osoiteryhmään kuuluvat kaikki IP-osoitteet väliltä 200.10.1.129 – 200.10.1.142. Tämän jälkeen konfiguroitiin samalla tavalla, kuin staattisen NAT:n tapauksessakin, mutta nyt viitattiin lopussa juuri luotuun osoiteryhmään.

set security nat proxy-arp interface ge-1/0/2.0 address 200.10.1.129/32 to 200.10.1.142/32

Lopuksi konfiguroitiin proxy-arp, rajapintaan ge-1/0/2.0 osoitteilla 200.10.1.129 - 200.10.1.142.

7.5 VPN-yhteyksien konfigurointi

7.5.1 Reittipohjainen VPN (route-based VPN)

Reittipohjaisen VPN-yhteyden konfigurointi suoritetaan monessa vaiheessa. Aluksi konfiguroidaan peruskonfiguraatiot, kuten rajapinnat, staattiset reitit, turva-alueet ja niiden osoitekirjat sekä lopuksi turvasäännöt. Vasta näiden jälkeen voidaan konfiguroida IKE sekä IPSec.

Aluksi määriteltiin rajapinta st0.0, joka on tässä VPN-yhteydessä käytetty tunneli, jonka jälkeen määriteltiin staattinen reitti verkkoon 192.168.3.128/25. Rajapinnalle täytyi myös muodostaa erillinen turva-alue. Alapuolella esimerkkinä Juniper-R5 laitteen konfiguraatioita:

```
interfaces {
   st0 {
      unit 0 {
         family inet {
            address 10.10.10.10/24;
         }
      }
   }
}
routing-options {
   static {
      route 192.168.3.128/25 next-hop st0.0;
   }
}
security {
   zones {
     security-zone vpn-wg3 {
        address-book {
           address wg3 192.168.3.128/25;
        }
        interfaces {
           st0.0;
         }

      }

   }

}
```

IKE avaintenvaihtoprosessin konfigurointi:

```
security {
   ike {
      proposal ike-phase1-proposal {
         authentication-method pre-shared-keys;
         dh-group group2;
         authentication-algorithm sha1;
         encryption-algorithm aes-128-cbc;
      }
   }
}
```

Aluksi konfiguroitiin ehdotus, jolle annettiin uniikki nimi, sekä määriteltiin autentikaatiomenetelmäksi *pre-shared-keys*, diffie-hellman ryhmäksi *group2*, autentikaatioalgoritmiksi *sha1* sekä tiedonsalaus-algoritmiksi *aes-128-cbc*.

```
      policy ike-phase1-policy {
         mode main;
         proposals ike-phase1-proposal;
         pre-shared-key ascii-text "$9$-uVYokqfz39GDnC"; ## SECRET-DATA
      }
```

Seuraavaksi konfiguroitiin sääntö *ike-phase1-policy*, joka sidottiin aikaisemmin tehtyyn ehdotukseen. Tässä määriteltiin myös yhteyden muodostamiseen käytettävä avain.

```
      gateway gw-wg3 {
         ike-policy ike-phase1-policy;
         address 200.10.3.1;
         external-interface ge-1/0/2.0;
      }
```

Lopuksi määriteltiin yhdyskäytävä *gw-wg3*, joka sidottiin sääntöön *ike-phase1-policy*. Yhdyskäytävälle määriteltiin laitteen ulospäin lähtevän liikenteen osoite 200.10.3.1 ja rajapinta ge-1/0/2.0.

Seuraavaksi konfiguroitiin IPSec:

```
   ipsec {
      proposal ipsec-phase2-proposal {
         protocol esp;
         authentication-algorithm hmac-sha1-96;
         encryption-algorithm aes-128-cbc;
      }
   }
```

Aluksi konfiguroitiin ehdotus, johon määriteltiin käytettäväksi protokolla *esp*, autentikointi algoritmi *hmac-sha1-96* sekä tiedonsalaus algoritmi *aes-128-cbc*.

```
policy ipsec-phase2-policy {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals ipsec-phase2-proposal;
}
```

Seuraavaksi luotiin sääntö *ipsec-phase2-policy*, johon määriteltiin käytettäväksi *perfect-forwarf-secrecy* ja Diffie-Hellman ryhmä *group2.* Tämän jälkeen sääntö sidottiin ehdotukseen.

```
vpn ike-vpn-wg3 {
    bind-interface st0.0;
    ike {
        gateway gw-wg3;
    }
}
```

Lopuksi luotiin VPN:lle nimi *ike-vpn-wg3*, joka sidottiin rajapintaan *st0.0* sekä aikaisemmin IKE-vaiheessa määriteltyyn yhdyskäytävään *gw-wg3.*

Tämän jälkeen määriteltiin vielä turvasäännöt turva-alueelta *wg1* alueelle *vpn-wg3* ja toisinpäin.

```
from-zone wg1 to-zone vpn-wg3 {
    policy vpn-wg1-wg3 {
        match {
            source-address wg1;
            destination-address wg3;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone vpn-wg3 to-zone wg1 {
    policy vpn-wg3-wg1 {
        match {
            source-address wg3;
            destination-address wg1;
```

```
            application any;
        }
        then {
            permit;
        }
    }
}
```

Turvasäännöt ovat yksinkertaiset, jossa määriteltiin vain lähde- ja kohdeosoitteet sekä sallittiin liikenne.

Täydelliset Juniper-R5 ja Juniper-R4 laitteiden konfiguraatiot reittipohjaisesta VPN:stä löytyy liitteistä 2 ja 6.

7.5.2 Sääntöpohjainen VPN (policy-based VPN)

Sääntöpohjaisen VPN:n konfigurointi tässä työssä toteutettiin samoilla IKE ja IPSec asetuksilla, kuin reittipohjaisessa VPN-yhteyden konfiguroinnissakin:

```
security {
    ike {
        proposal ike-phase1-proposal {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm aes-128-cbc;
        }
        policy ike-phase1-policy {
            mode main;
            proposals ike-phase1-proposal;
            pre-shared-key ascii-text "$9$g2JZjTQnCpBGDnC"; ## SECRET-DATA
        }
        gateway gw-wg3 {
            ike-policy ike-phase1-policy;
            address 200.10.3.1;
            external-interface ge-1/0/2.0;
        }
    }
    ipsec {
        proposal ipsec-phase2-proposal {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-128-cbc;
        }
        policy ipsec-phase2-policy {
            perfect-forward-secrecy {
```

```
            keys group2;
        }
        proposals ipsec-phase2-proposal;
    }
    vpn ike-vpn-wg3 {
        ike {
            gateway gw-wg3;
            ipsec-policy ipsec-phase2-policy;
        }
    }
}
```

Seuraavaksi konfiguroitiin säännöt:

```
policies {
    from-zone internet to-zone wg1 {
        policy vpn-3-1 {
            match {
                source-address wg3;
                destination-address wg1;
                application any;
            }
            then {
                permit {
                    tunnel {
                        ipsec-vpn ike-vpn-wg3;
                        pair-policy vpn-1-3;
                    }
                }
            }
        }
    }
    from-zone wg1 to-zone internet {
        policy vpn-1-3 {
            match {
                source-address wg1;
                destination-address wg3;
                application any;
            }
            then {
                permit {
                    tunnel {
                        ipsec-vpn ike-vpn-wg3;
                        pair-policy vpn-3-1;
                    }
                }
            }
        }
    }
}
```

Yläpuolella olevassa konfiguraatiossa määriteltiin lähde- ja kohdeosoitteet sekä määriteltiin liikenne menemään jo aikaisemmin luodun tunnelin *ike-vpn-wg3* kautta. Komennolla *pair-policy* sidotaan kaksi turvasääntöä, jotka käyttävät samaa VPN-tunnelia, käyttämään samaa SA:ta. Kaikki sääntöpohjaisen VPN-yhteyden konfiguraatiot löytyvät liitteistä 3 ja 7.

7.5.3 Reittipohjainen VPN Cisco Systemsin reitittimeen

VPN-yhteyden konfigurointi Juniper-R5 ja wg2-r1 -reitittimien välille suoritettiin reittipohjaisena VPN-yhteytenä. Juniper-R5 reitittimen konfiguraatio tehtiin samalla kaavalla, kuin kappaleessa 7.5.1. Aluksi käydään läpi vaihe yksi, eli IKE avaintenvaihtoprosessi molemmilla reitittimillä. Alapuolella WG2-R1-reitittimen IKE konfiguraatio.

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
 lifetime 300
crypto isakmp key “avain” address 200.10.1.1
```

Aluksi määriteltiin ISAKMP sääntö *10*. Tiedonsalausalgoritmiksi määriteltiin AES 256kb, autentikointimenetelmäksi *pre-share*, Diffie-Hellman algoritmin ryhmä 2 sekä ISAKMP avaintenvaihdon elinikä komennolla *lifetime*. Lopuksi määriteltiin ISAKMP-yhteydelle avain, sekä kohdeosoite *200.10.1.1*, joka on Juniper-R5-reitittimen vastaanottava rajapinta Ge-1/0/2.

Seuraavassa konfiguraatiossa Juniper-R5 reitittimen IKE asetukset:

```
ike {
   proposal ike-phase1-proposal {
      authentication-method pre-shared-keys;
      dh-group group2;
      authentication-algorithm sha1;
      encryption-algorithm aes-256-cbc;
      lifetime-seconds 300;
   }
   policy ike-phase1-policy {
      mode main;
      proposals ike-phase1-proposal;
      pre-shared-key ascii-text "$9$eAOW87g4ZjkPLxZj"; ## SECRET-DATA
   }
   gateway gw-cisco {
```

```
        ike-policy ike-phase1-policy;
        address 200.10.2.1;
        external-interface ge-1/0/2.0;
    }
}
```

Junos-käyttöjärjestelmässä konfiguraatio aloitettiin tekemällä ehdotus (proposal), johon määriteltiin autentikointityyli, Diffie-Hellman ryhmä, autentikointialgoritmi, tiedonsalausalgoritmi sekä IKE ehdotukselle elinikä. Näihin konfiguraatioihin asetettiin samat arvot, kuin reitittimeen WG2-R1. Mikäli yksikin arvo näistä olisi konfiguroitu poikkeavasti toisesta osapuolesta, ei avaintenvaihtoprosessia pystyttäisi onnistuneesti suorittamaan. Lopuksi määriteltiin vielä oletusyhdyskäytävän nimi, IP-osoite sekä neuvotteluun käytettävä ulkoinen rajapinta.

Kun avaintenvaihto on onnistuneesti suoritettu, konfiguroitiin IPSec VPN-yhteyden toinen osuus. Alapuolella WG2-R1-reitittimen konfiguraatio IPSec osuudesta:

```
crypto ipsec transform-set cisco esp-aes 256 esp-sha-hmac
crypto map cisco 10 ipsec-isakmp
 set peer 200.10.1.1
 set transform-set cisco
 set pfs group2
 match address 102
```

Konfigurointi aloitetaan määrittelemällä *transform-set*, johon määritellään. IPSec-yhteydelle määritellään käytettäväksi protokollaksi *esp,* tiedonsalausalgoritmiksi *aes 256* sekä autentikointialgoritmiksi *sha-hmac*. Tämän jälkeen sidotaan IPSec aikaisemmin luotuun ISAKMP sääntöön komennolla *crypto map cisco 10 ipsec-isakmp*. Edellisessä vaihesesa luotiin myös *crypto map* nimeltään cisco, johon liitetään *transform-set* cisco, määritellään yhteyden toisen osapuolen IP-osoite sekä asetetaan yhteys käyttämään Perfect Forward Secrecyä (PFS) Diffie-Hellman ryhmällä kaksi. Lopuksi määritellään vielä yhteys vertaamaan osoitteita Access Control List (ACL)-pääsylistaan 102. Pääsylistan konfigurointi alapuolella:

```
access-list 102 permit ip 192.168.2.128 0.0.0.127 192.168.1.128 0.0.0.127
```

Pääsylistassa 102 sallittiin yhteys reitittimeltä wg2-r1 reitittimeen Juniper-R5. Tämän jälkeen IPSec-yhteys sidottiin käytettävään rajapintaan GigabitEthernet0/0 sekä määriteltiin staattinen reititys.

```
interface GigabitEthernet0/0
 ip address 200.10.2.1 255.255.255.0
crypto map cisco
!
ip route 192.168.1.128 255.255.255.128 GigabitEthernet0/0
```

Seuraavana IPSec asetukset Juniper-R5 reitittimellä:

```
ipsec {
   proposal ipsec-phase2-proposal {
      protocol esp;
      authentication-algorithm hmac-sha1-96;
      encryption-algorithm aes-256-cbc;
      lifetime-seconds 300;
   }
   policy ipsec-phase2-policy {
      perfect-forward-secrecy {
         keys group2;
      }
      proposals ipsec-phase2-proposal;
   }
   vpn ike-vpn-cisco {
      bind-interface st0.0;
      ike {
         gateway gw-cisco;
         ipsec-policy ipsec-phase2-policy;
      }
   }
```

Yläpuolella olevassa konfiguraatiossa määriteltiin ensin ehdotus *ipsec-phase2-proposal*. Tämän jälkeen määriteltiin IPSec sääntö *ipsec-phase2*-policy, joka liitettiin ehdotukseen. Ehdotukseen ja sääntöön asetettiin samat asetukset, kuin WG2-R1 reitittimeenkin. Lopuksi luotiin VPN nimeltä *ike-vpn-cisco*, johon liitettiin rajapinnaksi *st0.0*, IKE yhdyskäytäväksi aikaisemmin luotu *gw-cisco* sekä sääntö *ipsec-phase2-policy*.

Juniper-R5 reitittimeen asetettiin rajapinta *st0.0* sekä staattinen reitti kulkemaan tämän rajapinnan kautta reitittimeen WG2-R1.

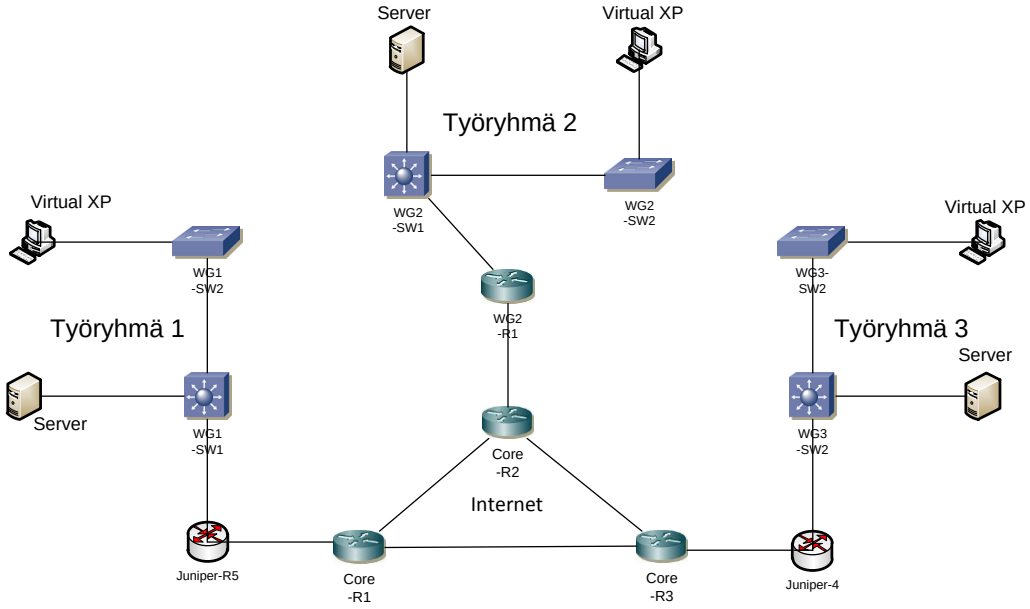
```
st0 {
    unit 0 {
        family inet {
            address 172.16.1.1/32;
        }
    }
}
routing-options {
    static {
        route 192.168.2.128/25 next-hop st0.0;
    }
}
```

Täydelliset konfiguraatiot VPN-yhteyden muodostamiseen löytyy liitteistä 4 ja 8.

8 Tulokset

8.1 Ympäristö

Työn tuloksena saatiin toimiva ympäristö, jossa tietoturvaominaisuuksien konfigurointi ja monipuolinen testaus oli mahdollista. Työssä simuloitiin ”Internetiä” sekä yrityksen kolmea toimipistettä. Suurin osa tietoturvaominaisuuksista testattiin toimipisteen yksi laitteella Juniper-R5.



KUVIO 33. Koko työn topologia

”Internetin” OSPF-reitityksen toiminta on esitetty kuviossa 34 käyttämällä show ip route -komentoa laitteella Core-R1.

```
Core-R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    200.10.1.0/24 is directly connected, FastEthernet3/2
O    200.10.2.0/24 [110/2] via 130.0.0.9, 19:21:42, FastEthernet3/0
O    200.10.3.0/24 [110/2] via 130.0.0.2, 19:21:42, FastEthernet3/1
     130.0.0.0/16 is variably subnetted, 6 subnets, 2 masks
C       130.0.3.0/30 is directly connected, Loopback0
C       130.0.0.0/30 is directly connected, FastEthernet3/1
O       130.0.5.1/32 [110/2] via 130.0.0.9, 19:21:42, FastEthernet3/0
O       130.0.0.4/30 [110/2] via 130.0.0.9, 19:21:42, FastEthernet3/0
                     [110/2] via 130.0.0.2, 19:21:43, FastEthernet3/1
O       130.0.4.1/32 [110/2] via 130.0.0.2, 19:21:43, FastEthernet3/1
C       130.0.0.8/30 is directly connected, FastEthernet3/0
Core-R1# _
```

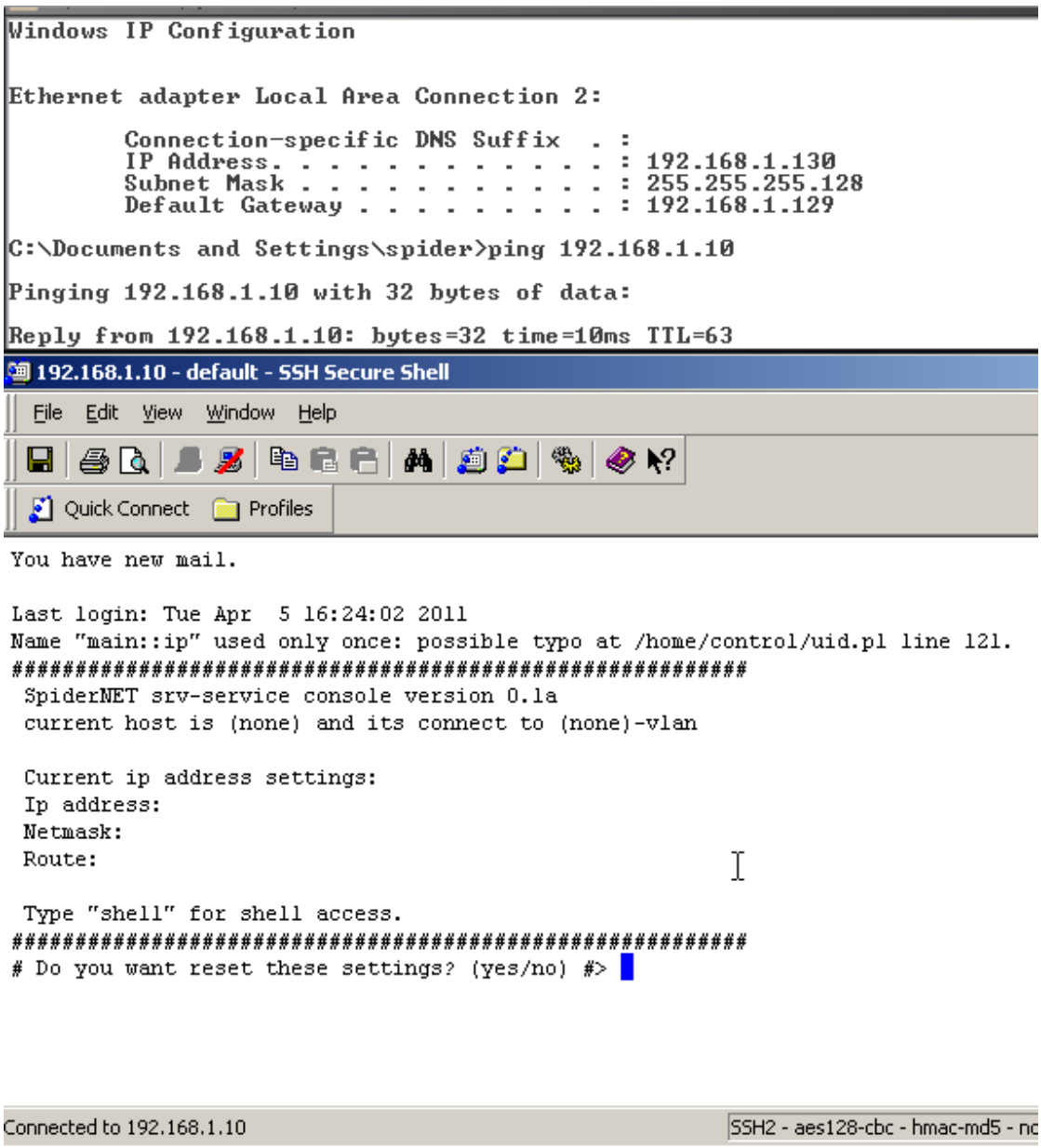
KUVIO 34. Show ip route -komento laitteelta Core-R1.

Yläpuolella olevassa kuviossa vasemmassa reunassa C:llä merkityt verkot tai osoitteet ovat Core-R1-reitittimen rajapinnassa suoraan yhteydessä, O:lla merkityt ovat OSPF reittejä, sekä S:llä merkityt ovat staattisia reittejä.

8.2 Turvasääntöjen (Security Policy) todentaminen

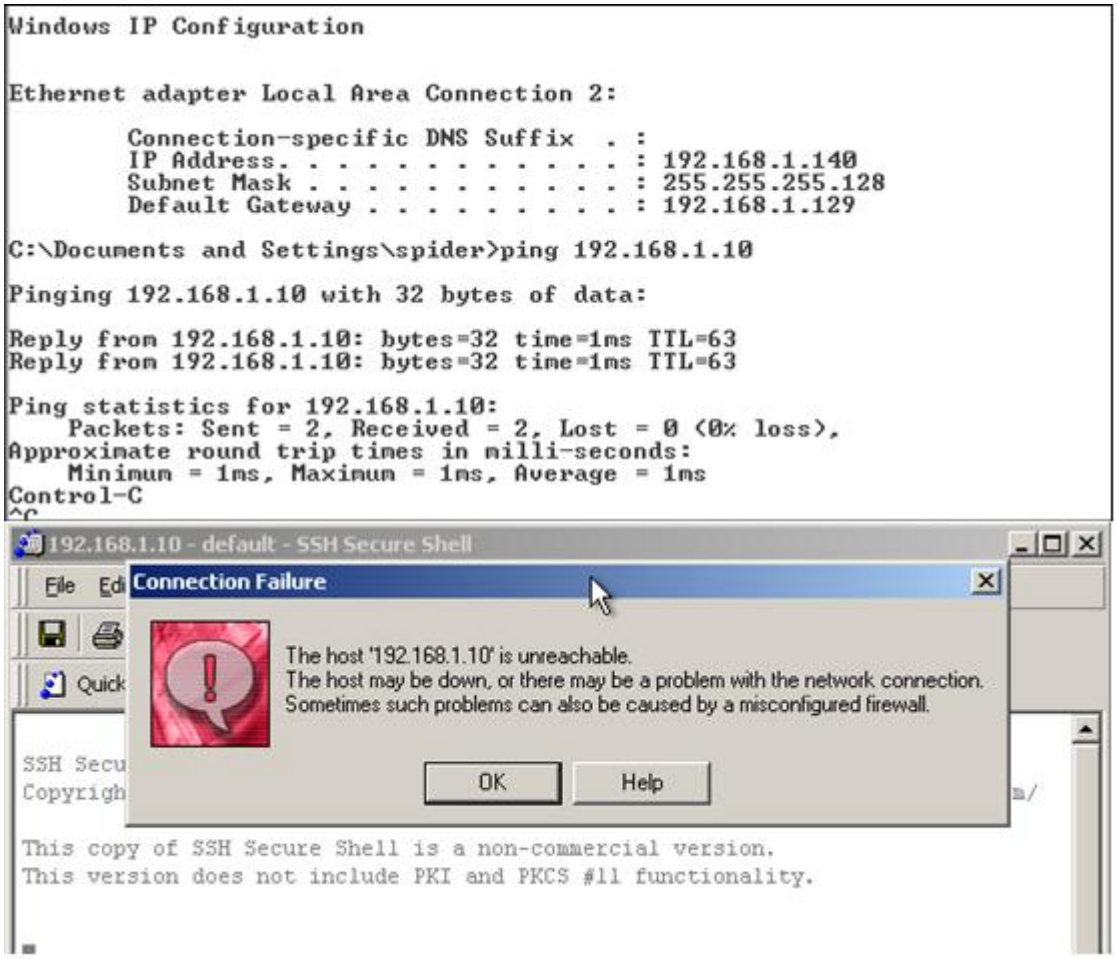
Turvasääntöjen toimivuutta testattiin työryhmässä yksi siten, että konfiguroitiin turva-alueen wg1 IP-osoitteet kahdenlaisille käyttäjille: normaali ja admin. Admin käyttäjä eroteltiin muista siten, että määriteltiin työryhmän osoitekirjaan (Address book) IP-osoite 192.168.1.130/32, jonka nimeksi määriteltiin admin. Loput käyttäjät lisättiin osoitekirjaan aliverkolla 192.168.1.129/25, nimellä wg1. Turva-alueelta *server* on sallittu kaikki liikenne kaikkiin osoitteisiin turva-alueelle *wg1*, joten näin päin ei liikennettä rajoitettu.

Turvasääntöihin määriteltiin ensin sääntö admin, johon sallittiin kaikki liikenne alueelta *wg1* alueelle *server*. Tämän jälkeen pystyttiin rajoittamaan muiden osoitteiden palveluita, kuten ping, ssh ja telnet. Kuviosta 35 näkyy, kuinka IP-osoitteesta 192.168.1.130 SSH Secure Shell -yhteyden ottaminen työryhmän palvelimeen onnistuu. Yhteys otettiin virtuaaliselta XP-koneelta virtuaaliseen palvelimeen.



KUVIO 35. Turvasääntöjen testaus IP-osoitteesta 192.168.1.130

Seuraavaksi vaihdoin XP-koneen IP-osoitteeksi 192.168.1.140 ja testasin samaa toimenpidettä. Kuviosta 36 näkyy, kuinka ssh-yhteyden muodostaminen ei onnistu.



KUVIO 36. Turvasäännön testaus IP-osoitteesta 192.168.1.140

8.3 NAT

8.3.1 Static NAT

Staattinen NAT määriteltiin vain työryhmässä yksi olevan palvelimen IP-osoitteelle 192.168.1.10, jonka julkiseksi osoitteeksi asetettiin 200.10.1.10. Core-R1 -reitittimeltä suoritettiin ping-komennolla testi palvelimen julkiseen IP-osoitteeseen. Kuviossa 37 on kuvankaappaus Juniper-R5 reitittimeltä komennosta *show security nat static rule all*, jossa kohta *Translation hits* näyttää, kuinka monta kertaa kyseistä osoitetta on muutettu.

```
Welcome to SpiderNet, press ENTER to continue

root@Juniper-R5> show security nat static rule all
Total static-nat rules: 1

Static NAT rule: r-static              Rule-set: rs-static
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : internet
  Destination addresses     : 200.10.1.10
  Host addresses            : 192.168.1.10
  Netmask                   : 255.255.255.255
  Host routing-instance     : N/A
  Translation hits          : 33427

root@Juniper-R5> _
```

KUVIO 37. Staattisen NAT:n osoitteenmuutoksien määrä

Kuviossa 38 on kuvankaappaus komennosta *show security flow session nat extensive*. Kuviosta nähdään, miten Core-R1:ltä lähetetty icmp-paketti käy osoitteenmuutoksen Juniper-R5 reitittimessä osoitteesta 200.10.1.10 osoitteeseen 192.168.1.10.

```
root@Juniper-R5> show security flow session nat extensive
Session ID: 16981, Status: Normal
Flag: 0x84000000
Policy name: 1/6
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 4
Session State: Valid
Start time: 2133500, Duration: 0
   In: 200.10.1.2/0 --> 200.10.1.10/40;icmp,
    Interface: ge-1/0/2.0,
    Session token: 0x200, Flag: 0x0x21
    Route: 0x70010, Gateway: 200.10.1.2, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 100
   Out: 192.168.1.10/40 --> 200.10.1.2/0;icmp,
    Interface: ge-1/0/7.10,
    Session token: 0x240, Flag: 0x0x30
    Route: 0x90010, Gateway: 192.168.1.10, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 100
Total sessions: 1

root@Juniper-R5>
```

KUVIO 38. Staattisen NAT:n istunnon tiedot

8.3.2 Lähde NAT

Lähde NAT testattiin pingaamalla työryhmän yksi virtuaalisesta työasemasta osoitetta 130.0.0.1, joka on rajapinta laitteessa CiscoCore-R1 (ks. kuvio 39).

```
Windows IP Configuration


Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.130
        Subnet Mask . . . . . . . . . . . : 255.255.255.128
        Default Gateway . . . . . . . . . : 192.168.1.129

C:\Documents and Settings\spider>ping 130.0.0.1

Pinging 130.0.0.1 with 32 bytes of data:

Reply from 130.0.0.1: bytes=32 time=2ms TTL=254
Reply from 130.0.0.1: bytes=32 time=2ms TTL=254
Reply from 130.0.0.1: bytes=32 time=5ms TTL=254
Reply from 130.0.0.1: bytes=32 time=6ms TTL=254

Ping statistics for 130.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 6ms, Average = 3ms

C:\Documents and Settings\spider>
```

KUVIO 39. Lähde NAT:n testaus.

Kuviossa 40 on kuvankaappaus komennoista *show security nat source rule.* Kuvankaappauksesta näkyy osoitealtaan (pool) määritelmät, säännön ID, mitä turva-alueita NAT koskee sekä kuinka monta kertaa osoitteenmuutoksia on tehty (kohta Translation hits).

```
root@Juniper-R5> show security nat source rule all
Total rules: 1

source NAT rule: r-source               Rule-set: rs-source
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : wg1
  To zone                   : internet
  Match
    Source addresses        : 192.168.1.128   - 192.168.1.255
    Destination addresses   : Any             - 255.255.255.255
    Destination port        : 0               - 0
  Action                      : pool1
    Persistent NAT type       : N/A
    Persistent NAT mapping type : address-port-mapping
    Inactivity timeout        : 0
    Max session number        : 0
  Translation hits          : 57

root@Juniper-R5> _
```

KUVIO 40. Lähde NAT säännön ominaisuudet.

Kuviosta 41 nähdään meneillään olevan NAT istunnon käytössä oleva osoiteallas (pool) sekä istunnossa tapahtuva osoitteenmuutos. Tässä tapauksessa yksityinen osoite 192.168.1.130 vaihdetaan julkiseen osoitteeseen 200.10.1.131.

```
root@Juniper-R5> show security flow session nat extensive
Session ID: 16965, Status: Normal
Flag: 0x80000000
Policy name: 1/14
Source NAT pool: pool1
Maximum timeout: 4, Current timeout: 2
Session State: Valid
Start time: 2133403, Duration: 2
   In: 192.168.1.130/8451 --> 130.0.0.1/512;icmp,
    Interface: ge-1/0/7.20,
    Session token: 0x280, Flag: 0x0x21
    Route: 0x80010, Gateway: 192.168.1.130, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 60
   Out: 130.0.0.1/512 --> 200.10.1.131/27998;icmp,
    Interface: ge-1/0/2.0,
    Session token: 0x200, Flag: 0x0x20
    Route: 0x70010, Gateway: 200.10.1.2, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 60
```

KUVIO 41. Lähde NAT istunnon ominaisuudet.

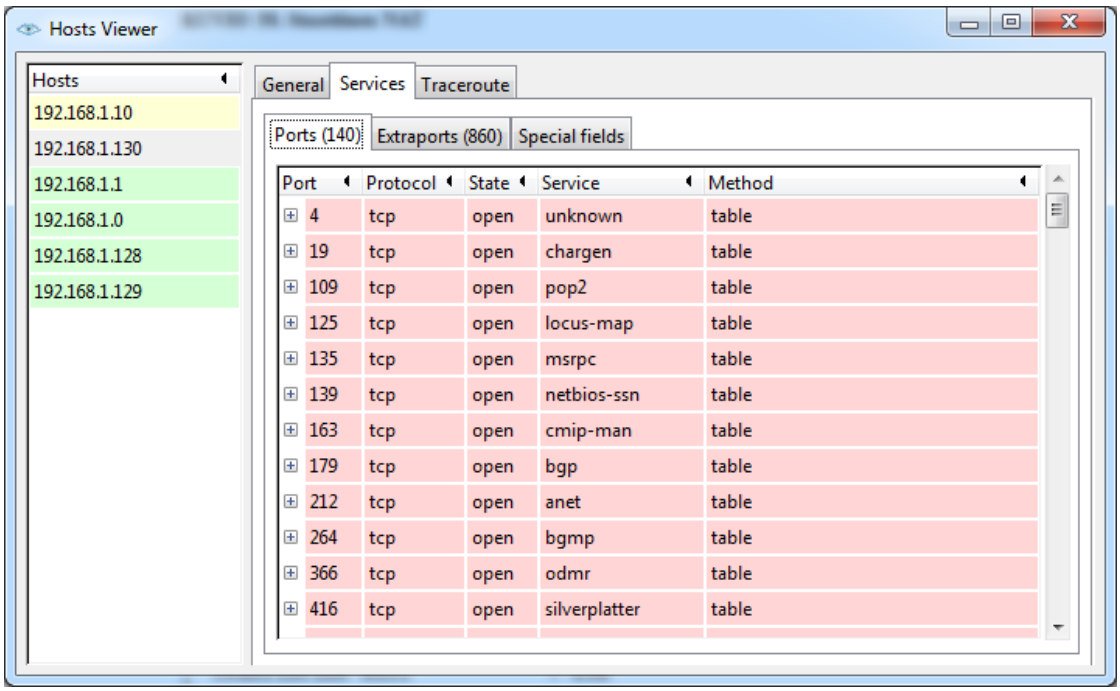
8.4 Screenit

8.4.1 Testaustapa

Screenien testaus suoritettiin NMAP – Zenmap GUI verkon skannaus ohjelmalla ja ping-komennon erikoistoiminnoilla. NMAP-ohjelmalla luotiin porttiskannauksia, joita yritettiin Junos-käyttöjärjestelmän ominaisuuksilla estää. NMAP-ohjelmaa käytettiin Windows XP-koneella, joka oli kiinni Core-R2 –reitittimessä, rajapinnassa FastEthernet 3/10.

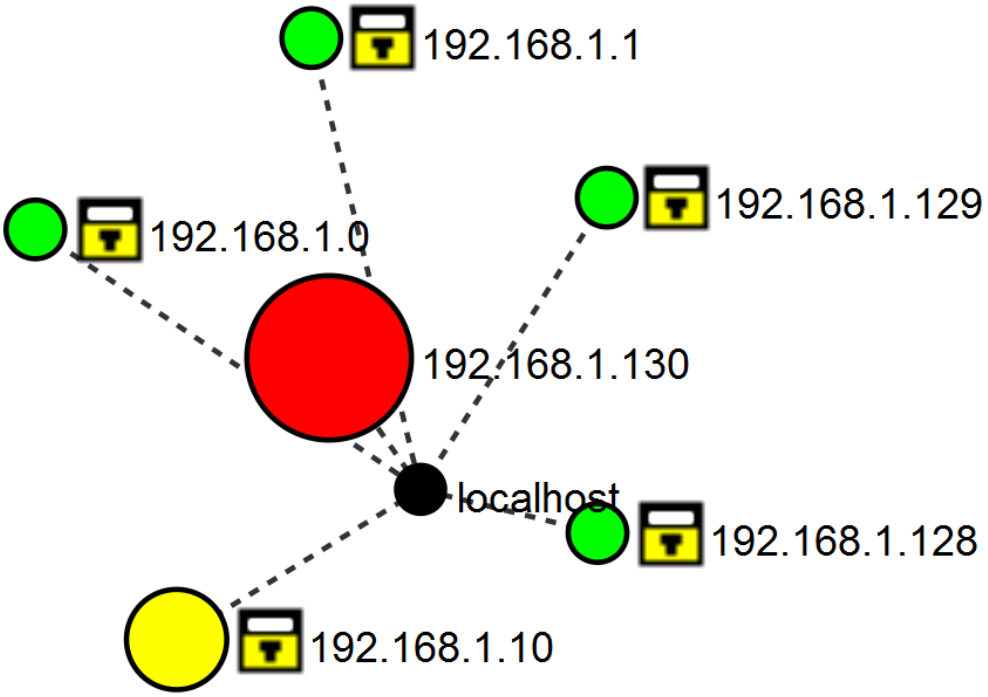
8.4.2 Porttiskannaus

Aluksi testattiin, mitä NMAP porttiskannerilla saadaan selville, kun käytettiin NMAP:ssa valmiiksi olevaa *regular scan* -vaihtoehtoa. Skannaus kohdistettiin osoitteeseen 192.168.1.0/24, josta saatiin selville kaikki loppukäyttäjät (ks. kuvio 42), osan topologiasta (ks. kuvio 43.) ja suuren listan palveluita selville kultakin loppukäyttäjältä (ks. kuvio 42).



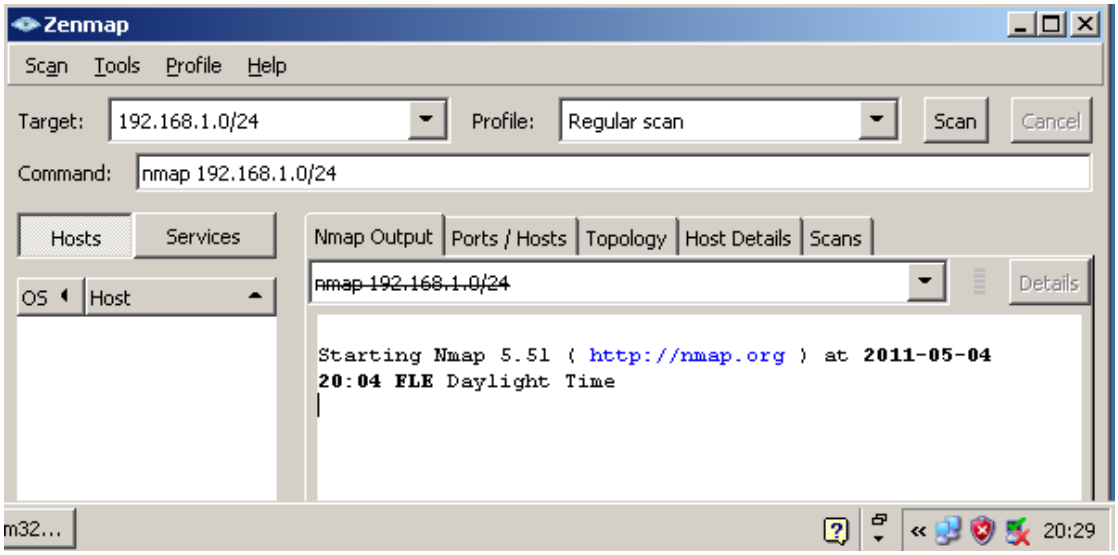
KUVIO 42. NMAP Regular scan, ilman Screenejä.

Yläpuolella olevassa kuviossa on vasemmassa reunassa lueteltu laitteiden IP-osoitteet, joista käyttäjän valitsemalla, saa selville kyseisen loppukäyttäjän tai laitteen porttien tilat ja palvelut. Kuviossa 43 on NMAP skannauksella selvitetty topologia, jossa on työryhmän yksi kaikki laitteiden IP-osoitteet.



KUVIO 43. NMAP skannaus, selville saatu topologia.

Junos-käyttöjärjestelmän Screeni port-scan 5000 aktivoitiin, mutta siitä ei ollut mitään hyötyä, sillä samat tulokset saatiin selville NMAP -ohjelmalla, vaikka Screeni oli päällä. Kun port-scan Screenin threshold arvoa vaihdettiin isommaksi, alkoi tulosta tulla. Kun arvoksi laitettiin 1000000, ei NMAP –ohjelma enää pystynyt tekemään porttiskannausta. Kuviosta 44 nähdään, kuinka NMAP ei onnistunut suorittamaan skannausta 25 minuutissa, jolloin skannaus keskeytettiin.



KUVIO 44. Port-scan Screen toimii.

Junos-käyttöjärjestelmä rekisteröi kaikki port-scan yritykset, mikäli *port-scan* Screen on päällä (ks. kuvio 45).

```
root@Juniper-R5> show security screen ids-option testi
Screen object status:

Name                                            Value
  TCP port scan threshold                       1000000

root@Juniper-R5> show security screen statistics zone internet
Screen statistics:

IDS attack type                                 Statistics
  ICMP flood                                    0
  UDP flood                                     0
  TCP winnuke                                   0
  TCP port scan                                 17984
  ICMP address sweep                            0
  TCP sweep                                     0
  UDP sweep                                     0
  IP tear drop                                  0
  TCP SYN flood                                 0
  IP spoofing                                   0
  ICMP ping of death                            0
  IP source route option                        0
  TCP land attack                               0
  TCP SYN fragment                              0
  TCP no flag                                   0
  IP unknown protocol                           0
  IP bad options                                0
  IP record route option                        0
  IP timestamp option                           0
  IP security option                            0
  IP loose source route option                  0
  IP strict source route option                 0
  IP stream option                              0
  ICMP fragment                                 0
  ICMP large packet                             0
  TCP SYN FIN                                   0
  TCP FIN no ACK                                0
  Source session limit                          0
  TCP SYN-ACK-ACK proxy                         0
  IP block fragment                             0
  Destination session limit                     0

root@Juniper-R5>
```

KUVIO 45. Port-scan Screen.

8.4.3 ICMP-Large

Toinen Screen, jota testattiin, oli ICMP-large. Kohteeseen 192.168.1.10, eli palvelimen IP-osoitteeseen lähetettiin ylisuuria ICMP-paketteja, jonka Junos käyttöjärjestelmän Screen ICMP-large esti. Kuviossa 46 kohdassa ICMP large packet on rekisteröity ylisuuret ICMP paketit, jotka on tullut kuvion 47 mukaisista pingaus yrityksistä.

```
root@Juniper-R5> show security screen ids-option testi
Screen object status:

Name                                                Value
  ICMP large packet                                 enabled

root@Juniper-R5> show security screen statistics zone internet
Screen statistics:

IDS attack type                                     Statistics
  ICMP flood                                        0
  UDP flood                                         0
  TCP winnuke                                       0
  TCP port scan                                     0
  ICMP address sweep                                0
  TCP sweep                                         0
  UDP sweep                                         0
  IP tear drop                                      0
  TCP SYN flood                                     0
  IP spoofing                                       0
  ICMP ping of death                                0
  IP source route option                            0
  TCP land attack                                   0
  TCP SYN fragment                                  0
  TCP no flag                                       0
  IP unknown protocol                               0
  IP bad options                                    0
  IP record route option                            0
  IP timestamp option                               0
  IP security option                                0
  IP loose source route option                      0
  IP strict source route option                     0
  IP stream option                                  0
  ICMP fragment                                     0
  ICMP large packet                                 30
  TCP SYN FIN                                       0
  TCP FIN no ACK                                    0
  Source session limit                              0
  TCP SYN-ACK-ACK proxy                             0
  IP block fragment                                 0
  Destination session limit                         0

root@Juniper-R5>
```

KUVIO 46. ICMP-Large Screen todennus

```
C:\WINDOWS\system32\cmd.exe

Ping statistics for 172.16.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 192.168.1.10 -t -l 1500

Pinging 192.168.1.10 with 1500 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 15, Received = 0, Lost = 15 (100% loss),
Control-C
^C
```

KUVIO 47. Pingaus yritys, kun ICMP-Large Screen on aktivoituna

8.4.4 Fragmentoituneen IP-paketin torjuminen

Seuraavaksi testattiin fragmentoituneen IP-paketin torjumista. NMAP-ohjelmalla lähetettiin skannaus, jossa lähetettiin fragmentoituneita IP-paketteja. Junos-käyttöjärjestelmän Screenillä IP block fragmented saatiin paketit estettyä. Kuviossa 48 näkyy, kuinka Screen rekisteröi 40500 fragmentoitunutta IP-pakettia. Kuviossa olevat 30 ylisuurta ICMP-pakettia ei kuulunut tähän testiin, vaan johtuivat aikaisemmasta ICMP-large testistä.

```
[edit security screen ids-option testi]
root@Juniper-R5# show
icmp {
    large;
}

Name                                            Value
  TCP SYN fragment                              enabled
  ICMP large packet                             enabled
  IP block fragment                             enabled

root@Juniper-R5> show security screen statistics zone internet
Screen statistics:

IDS attack type                                 Statistics
  ICMP flood                                    0
  UDP flood                                     0
  TCP winnuke                                   0
  TCP port scan                                 0
  ICMP address sweep                            0
  TCP sweep                                     0
  UDP sweep                                     0
  IP tear drop                                  0
  TCP SYN flood                                 0
  IP spoofing                                   0
  ICMP ping of death                            0
  IP source route option                        0
  TCP land attack                               0
  TCP SYN fragment                              0
  TCP no flag                                   0
  IP unknown protocol                           0
  IP bad options                                0
  IP record route option                        0
  IP timestamp option                           0
  IP security option                            0
  IP loose source route option                  0
  IP strict source route option                 0
  IP stream option                              0
  ICMP fragment                                 0
  ICMP large packet                             30
  TCP SYN FIN                                   0
  TCP FIN no ACK                                0
  Source session limit                          0
  TCP SYN-ACK-ACK proxy                         0
  IP block fragment                             40500
  Destination session limit                     0
```

KUVIO 48. IP block fragment - Screen

8.5 VPN

8.5.1 Reittipohjainen VPN

Reittipohjaisen VPN–yhteyden testaaminen tapahtui käyttämällä ping -komentoa laitteiden Juniper-R5 ja Juniper-R4 välillä. Kuviosta 49 näemme, kuinka pingaus onnistuu.

```
root@Juniper-R5# run ping 192.168.3.129
PING 192.168.3.129 (192.168.3.129): 56 data bytes
^C
--- 192.168.3.129 ping statistics ---
1 packets transmitted, 0 packets received, 100% packet loss

[edit]
root@Juniper-R5# run ping 192.168.3.129 source 192.168.1.129
PING 192.168.3.129 (192.168.3.129): 56 data bytes
64 bytes from 192.168.3.129: icmp_seq=0 ttl=64 time=10.937 ms
64 bytes from 192.168.3.129: icmp_seq=1 ttl=64 time=4.439 ms
64 bytes from 192.168.3.129: icmp_seq=2 ttl=64 time=6.491 ms
64 bytes from 192.168.3.129: icmp_seq=3 ttl=64 time=6.061 ms
64 bytes from 192.168.3.129: icmp_seq=4 ttl=64 time=3.351 ms
^C
--- 192.168.3.129 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.351/6.256/10.937/2.598 ms

[edit]
root@Juniper-R5# _
```

KUVIO 49. Reittipohjaisen VPN-yhteyden testaus.

Kuviossa 50 on ike turva-assosiaatioiden (SA) tiedot.

```
root@Juniper-R5> show security ike security-associations detail
IKE peer 200.10.3.1, Index 39,                    1
  Role: Responder, State: UP
  Initiator cookie: 9e37556be30f8654, Responder cookie: 795e675dbfab8b04
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 200.10.1.1:500, Remote: 200.10.3.1:500                          2
  Lifetime: Expires in 22803 seconds
  Algorithms:
   Authentication        : sha1
   Encryption            : aes-cbc (128 bits)                    3
   Pseudo random function: hmac-sha1
  Traffic statistics:
   Input  bytes  :                 2040
   Output bytes  :                 1852
   Input  packets:                   11                          4
   Output packets:                    8
  Flags: Caller notification sent
  IPSec security associations: 3 created, 2 deleted
  Phase 2 negotiations in progress: 1                             5

    Negotiation type: Quick mode, Role: Responder, Message ID: 1999561482
    Local: 200.10.1.1:500, Remote: 200.10.3.1:500
    Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    Flags: Caller notification sent, Waiting for done


root@Juniper-R5> _
```

KUVIO 50. IKE SA:n tiedot

Kuvio 50 on jaettu viiteen pienempään osaan joista selviää seuraavia tietoja:

1. Toisen IKE osapuolen yhdyskäytävän IP-osoite, SA:n indeksi numero, rooli sekä SA:n yhteyden tila.
2. Avaimenvaihtotyyli, autentikointityyli, paikallinen ja etä yhdyskäytävän osoite sekä SA:n voimassaoloaika.
3. Käytössä olevat algoritmit.
4. Liikenteen statistiikkaa
5. Tietoa luoduista ja käytössäolevista IPsec SA:sta.

Kuviossa 51 on IPSec turva-assosiaation tiedot. Merkityssä kohdassa näkyy käytössä oleva protokolla, autentikointi algoritmi sekä tiedonsalaus algoritmi.

```
root@Juniper-R5> show security ipsec security-associations detail
  Virtual-system: root
  Local Gateway: 200.10.1.1, Remote Gateway: 200.10.3.1
  Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    DF-bit: clear
    Direction: inbound, SPI: 5715bf27, AUX-SPI: 0
                                , VPN Monitoring: UP
    Hard lifetime: Expires in 283 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expired
    Mode: tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
```

KUVIO 51. IPSec SA:n tiedot

Kuviossa 52 on kuvankaappaus IPSec:stä, jossa näkyy eri protokollien tiedonsiirron tilastot sekä mahdollisten ongelmapakettien määrän.

```
root@Juniper-R5> show security ipsec statistics index ?
Possible completions:
  <index>              Index of Security Association
root@Juniper-R5> show security ipsec statistics
ESP Statistics:
  Encrypted bytes:           204288
  Decrypted bytes:           140364
  Encrypted packets:           1344
  Decrypted packets:           1671
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0

root@Juniper-R5> _
```

KUVIO 52. IPSec tilastot.

Kuviossa 53 on tiedot meneillään olevista istunnoista. Kuviosta selviää istuntojen ID, istunnon tila, aloitusaika, mahdollinen käytössä oleva sääntö, istunnon alkamisajankohta sekä kesto. Kuvankaappauksen hetkellä istuntoja on ollut toiminnassa kaksi.

```
root@Juniper-R5> show security flow session extensive
Session ID: 19990, Status: Normal
Flag: 0x10000
Policy name: N/A
Source NAT pool: Null
Maximum timeout: N/A, Current timeout: N/A
Session State: Valid
Start time: 2360479, Duration: 554
   In: 200.10.3.1/5372 --> 200.10.1.1/55049;esp,
    Interface: ge-1/0/2.0,
    Session token: 0x200, Flag: 0x0x4000621
    Route: 0x70010, Gateway: 200.10.1.2, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0

Session ID: 19991, Status: Normal
Flag: 0x10000
Policy name: N/A
Source NAT pool: Null
Maximum timeout: N/A, Current timeout: N/A
Session State: Valid
Start time: 2360479, Duration: 554
   In: 200.10.3.1/0 --> 200.10.1.1/0;esp,
    Interface: ge-1/0/2.0,
    Session token: 0x200, Flag: 0x0x621
    Route: 0x70010, Gateway: 200.10.1.2, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 2

root@Juniper-R5>
```

KUVIO 53. Istuntojen tiedot.

8.5.2 Sääntöpohjainen VPN

Sääntöpohjaisen VPN:n testaus suoritettiin ping –komentoa käyttäen eri työryhmien virtuaalisilta työasemilta (ks. kuvio 54).

```
Windows IP Configuration

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.130
        Subnet Mask . . . . . . . . . . . : 255.255.255.128
        Default Gateway . . . . . . . . . : 192.168.1.129

C:\Documents and Settings\spider>ping 192.168.3.130

Pinging 192.168.3.130 with 32 bytes of data:

Reply from 192.168.3.130: bytes=32 time=5ms TTL=127
Reply from 192.168.3.130: bytes=32 time=5ms TTL=127
Reply from 192.168.3.130: bytes=32 time=5ms TTL=127
Reply from 192.168.3.130: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.3.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 4ms

C:\Documents and Settings\spider>
```

KUVIO 54. Sääntöpohjaisen VPN–yhteyden testaus.

Kuviossa 55 näkyy IKE SA:n tiedot. Kuviosta selviää IKE osapuolten IP-osoitteet, indeksi numero, avaimenvaihtoprosessin tiedot, algoritmit, tilastot sekä aktiiviset vaiheen kaksi IPSec neuvottelut.

```
root@Juniper-R5> show security ike security-associations detail
IKE peer 200.10.3.1, Index 1,
  Role: Responder, State: UP
  Initiator cookie: 86d6ea1e0790f9bc, Responder cookie: 9ce31d41bbba7ef2
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 200.10.1.1:500, Remote: 200.10.3.1:500
  Lifetime: Expires in 24900 seconds
  Algorithms:
   Authentication        : sha1
   Encryption            : aes-cbc (128 bits)
   Pseudo random function: hmac-sha1
  Traffic statistics:
   Input  bytes  :                 1524
   Output bytes  :                 1364
   Input  packets:                    8
   Output packets:                    6
  Flags: Caller notification sent
  IPSec security associations: 2 created, 2 deleted
  Phase 2 negotiations in progress: 0

root@Juniper-R5>
```

KUVIO 55. IKE SA:n tiedot.

Kuviosta 56 on IPSec SA:n tiedot. Kuviosta selviää paikallinen yhdyskäytävä (Local Gateway) ja etäyhdyskäytävä (Remote Gateway). Lisäksi kohdasta *Policy-name* nähdään kyseisen SA:n käytössä oleva säännön nimi. Kuvion lopussa on käytössä oleva protokolla, autentikointialgoritmi sekä tiedonsalausalgoritmit.

```
root@Juniper-R5> show security ipsec security-associations detail
  Virtual-system: root
  Local Gateway: 200.10.1.1, Remote Gateway: 200.10.3.1
  Local Identity: ipv4_subnet(any:0,[0..7]=192.168.1.128/25)
  Remote Identity: ipv4_subnet(any:0,[0..7]=192.168.3.128/25)
    DF-bit: clear
    Policy-name: vpn-1-3

    Direction: inbound, SPI: 8132fac8, AUX-SPI: 0
                                , VPN Monitoring: -
    Hard lifetime: Expires in 1690 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 1082 seconds
    Mode: tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
```

KUVIO 56. IPSec SA:n tiedot.

Kuviossa 57 on kuvankaappaus komennosta *show security flow session*. Tällä komennolla nähdään käynnissä olevien istuntojen tiedot. Istuntoja kuvankaappaushetkellä on viisi.

```
root@Juniper-R5> show security flow session
Session ID: 18650, Policy name: N/A, Timeout: N/A, Valid
  In: 200.10.3.1/33074 --> 200.10.1.1/64200;esp, If: ge-1/0/2.0, Pkts: 0, Bytes:
 0

Session ID: 18651, Policy name: N/A, Timeout: N/A, Valid
  In: 200.10.3.1/0 --> 200.10.1.1/0;esp, If: ge-1/0/2.0, Pkts: 0, Bytes: 0

Session ID: 19143, Policy name: vpn-1-3/16, Timeout: 2, Valid
  In: 192.168.1.130/11523 --> 192.168.3.130/512;icmp, If: ge-1/0/7.20, Pkts: 1,
Bytes: 60
  Out: 192.168.3.130/512 --> 192.168.1.130/11523;icmp, If: ge-1/0/2.0, Pkts: 1,
Bytes: 60

Session ID: 19145, Policy name: vpn-1-3/16, Timeout: 2, Valid
  In: 192.168.1.130/12035 --> 192.168.3.130/512;icmp, If: ge-1/0/7.20, Pkts: 1,
Bytes: 60
  Out: 192.168.3.130/512 --> 192.168.1.130/12035;icmp, If: ge-1/0/2.0, Pkts: 1,
Bytes: 60

Session ID: 19146, Policy name: vpn-1-3/16, Timeout: 2, Valid
  In: 192.168.1.130/11779 --> 192.168.3.130/512;icmp, If: ge-1/0/7.20, Pkts: 1,
Bytes: 60
  Out: 192.168.3.130/512 --> 192.168.1.130/11779;icmp, If: ge-1/0/2.0, Pkts: 1,
Bytes: 60
Total sessions: 5

root@Juniper-R5>
```

KUVIO 57. Istuntojen tiedot.

8.5.3 VPN yhteys Cisco Systemsin reitittimeen

VPN-yhteydeys Cisco Systemsin ja Juniper Networksin reitittimien välillä testattiin ping-komentoa käyttäen. Kuviossa 58 näkyy kuvakaappaukset komennoista *show crypto isakmp policy* sekä *show crypto isakmp sa detail*. Ylemmässä osassa näkyy sääntöön määritellyt algoritmit, autentikointityyli, Diffie-Hellman ryhmä sekä säännön elinikä. Kuvion alareunasta nähdään, osapuolten yhdyskäytävät sekä kohdan *status* arvo *ACTIVE* osoittaa sen, että ISAKMP avaintenvaihto on onnistunut.

```
wg2-r1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys
).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               300 seconds, no volume limit
wg2-r1#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local            Remote           I-VRF      Status Encr Hash Auth DH Lifetime
 Cap.

1034  200.10.2.1       200.10.1.1                  ACTIVE aes  sha  psk  2  00:00:16

       Engine-id:Conn-id =  SW:34

IPv6 Crypto ISAKMP SA
```

KUVIO 58. Avaimenvaihtoprosessi laitteelta WG2-R1.

Kuviossa 59 on vastaavasti tiedot Juniper-R5 reitittimen SA tiedot. Kuvion ensimmäisessä osuudesta nähdään IKE SA:n rooli, tila, autentikointityyli, paikallisen- ja etäyhdyskäytävän IP-osoitteet sekä SA:n jäljellä oleva aika. Toisesta osuudesta selviää käytössä olevat algoritmit sekä liikenteen statistiikat. Kohdan *Traffic statistics* arvoista voidaan todeta, että IKE SA toimii. Kolmannesta osuudesta nähdään, että IPSec SA on luotu.

```
root@Juniper-R5> show security ike security-associations detail
IKE peer 200.10.2.1, Index 1217,
  Role: Initiator, State: UP
  Initiator cookie: da3f0a79779f6443, Responder cookie: 3055f771c786e167
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 200.10.1.1:500, Remote: 200.10.2.1:500
  Lifetime: Expires in 197 seconds
  Algorithms:
   Authentication        : sha1
   Encryption            : aes-cbc (256 bits)
   Pseudo random function: hmac-sha1
  Traffic statistics:
   Input  bytes  :                 1596
   Output bytes  :                 3764
   Input  packets:                   13
   Output packets:                   12
  Flags: Caller notification sent
  IPSec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 1

    Negotiation type: Quick mode, Role: Responder, Message ID: 3018209996
    Local: 200.10.1.1:500, Remote: 200.10.2.1:500
    Local identity: ipv4_subnet(any:0,[0..7]=192.168.1.128/25)
    Remote identity: ipv4_subnet(any:0,[0..7]=192.168.2.128/25)
    Flags: Caller notification sent, Waiting for done


root@Juniper-R5>
```

KUVIO 59. Avaimenvaihtoprosessi laitteelta Juniper-R5.

Kuviossa 60 on kuvankaappaus reitittimeltä WG2-R1 komennosta *show crypto ipsec sa detai*. Kuvion ensimmäisestä osiosta nähdään, että paketteja on käsitelty IPSec määritysten mukaisesti. Osiosta kaksi nähdään IPSec yhteyden paikallinen- ja etäyhdyskäytävä sekä aikaisemmin määritellyt ominaisuudet, kuten PFS ja Diffie-Hellman ryhmä. Kolmannessa osiossa näkyy, että IPSec tila on aktiivinen kohdasta *Status: ACTIVE*.

```
wg2-r1#show crypto ipsec sa detail

interface: GigabitEthernet0/0
    Crypto map tag: cisco, local addr 200.10.2.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.2.128/255.255.255.128/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.128/255.255.255.128/0/0)
   current_peer 200.10.1.1 port 500
     PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}
     #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
     #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #pkts no sa (send) 1, #pkts invalid sa (rcv) 0
     #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 2
     #pkts invalid prot (recv) 0, #pkts verify failed: 0
     #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
     #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
     ##pkts replay failed (rcv): 0
     #pkts internal err (send): 0, #pkts internal err (recv) 0

     local crypto endpt.: 200.10.2.1, remote crypto endpt.: 200.10.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0x2B18D40B(723047435)
     PFS (Y/N): Y, DH group: group2

     inbound esp sas:
      spi: 0x5999C77(93953143)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2039, flow_id: NETGX:39, sibling_flags 80000046, crypto map: ci
sco
        sa timing: remaining key lifetime (k/sec): (4590903/284)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:
```

KUVIO 60. Tiedot WG2-R1 käyttämästä IPSec SA:sta.

Kuviossa 61 on tiedot Juniper-R5 reitittimen IPSec SA:sta. Kuviosta selviää yhdyskäytävät, yhteyden elinaika, protokolla sekä autentikointi ja tiedonsalaus algoritmit.

```
root@Juniper-R5> show security ipsec security-associations detail
  Virtual-system: root
  Local Gateway: 200.10.1.1, Remote Gateway: 200.10.2.1
  Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    DF-bit: clear
    Direction: inbound, SPI: cb19795b, AUX-SPI: 0
                                , VPN Monitoring: UP
    Hard lifetime: Expires in 284 seconds
    Lifesize Remaining:  943710 kilobytes
    Soft lifetime: Expires in 236 seconds
    Mode: tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
```

KUVIO 61. IPSec SA tiedot reitittimeltä Juniper-R5

Kuviossa 62 on kuvankaappaus komennosta *show crypto session detail*, josta nähdään, että VPN-yhteys on aktiivinen.

```
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
Uptime: 00:00:04
Session status: UP-ACTIVE
Peer: 200.10.1.1 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 200.10.1.1
      Desc: (none)
  IKE SA: local 200.10.2.1/500 remote 200.10.1.1/500 Active
          Capabilities:(none) connid:1466 lifetime:00:03:13
  IPSEC FLOW: permit ip 192.168.2.128/255.255.255.128 192.168.1.128/255.255.255.
128
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 27 drop 20 life (KB/Sec) 4401136/295
        Outbound: #pkts enc'ed 30 drop 3 life (KB/Sec) 4401136/295

wg2-r1#
```

KUVIO 62. IPSec VPN tiedot reitittimeltä WG2-R1

9 Yhteenveto

9.1 Opinnäytetyön tekeminen

Opinnäytetyön yksi haastavimmista kohdista tuli vastaan heti alussa, sillä aikaisempaa kokemusta Juniperi Networksin reitittimistä, eikä Junos-käyttöjärjestelmästä ollut ollenkaan. Tämän takia työn tekeminen aloitettiin ottamalla kirja käteen ja opiskelemalla perusasiat Juniper Networksin reitittimistä sekä Junos-käyttöjärjestelmästä. Työn aloituksen yhteydessä sain pikaisen peruskoulutuksen Junos-käyttöjärjestelmästä toimeksiantajan edustajan, Marko Vatasen toimesta. Muihin työssä käytettäviin laitteisiin oltiin tutustuttu jo tietoverkkotekniikan koulutusohjelman opintojaksoilla, mutta työn edetessä totesin, että myös tutummista laitteista löytyi paljon uutta opittavaa.

Kun perusasiat olivat hallussa, aloitettiin työn topologian rakentaminen. Tässä vaiheessa itse tietoturvaominaisuudet jäivät vielä taka-alalle ja keskityttiin testausympäristön tekemiseen.

Testausympäristön valmistumisen jälkeen aloitettiin tietoturvaominaisuuksiin tutustuminen konfiguraatio tasolla. Tietoturvaominaisuuksista ensimmäisenä vastaan tulleet turva-alueet sekä turvasäännöt olivat positiivinen yllätys ja viimeinkin tässä vaiheessa alkoi Juniper-reitittimien toimintaperiaate selvitä. Yllätyin siitä, kuinka loogista Junos-käyttöjärjestelmän tapa käsitellä konfiguraatioita lopulta oli.

Työn mielenkiintoisin vaihe oli ehdottomasti Intrusion Detection and Prevention (IDP) -ominaisuudet eli Screenit. Screenien testaaminen NMAP-ohjelmalla oli mieltä avartavaa, kun näki mitä kaikkea yhdellä porttiskannauksella saatiin selville, jos verkkoa ei oltu suojattu hyökkäyksiltä. Tässä vaiheessa ongelmaksi osoittautui myös NMAP-ohjelman hyvyys, koska hyökkäyksien torjuminen ei onnistunutkaan ihan yhtä nappia painamalla vaan siihen jouduttiin uhraamaan tunteja, ennen kuin ensimmäinenkään porttiskannaus oli torjuttu.

VPN-yhteyksien muodostamisen yhteydessä havaittiin ongelma, joka oli ollut koko työn ajan ”Internetin” peruskonfiguraatiossa: työryhmien reunareitittimien mainostaminen Core-reitittimien OSPF-konfiguraatiossa oli jäänyt pois. Tästä oli seurauksena jo suoritettujen testauksien uudelleen suorittaminen. Tämän jälkeen IPSec VPN -

yhteydet toimivat lukuunottamatta yhteyttä työryhmän yksi (Juniper) ja kaksi (Cisco Systems) välillä. Tähän ongelmaan saatiin ratkaisu vasta sitten, kun kokoonnuttiin toimeksiantajan edustajan sekä työn ohjaajan kanssa asiaa miettimään. Ongelmana ei ollut reitittimien yhteensopivuus ongelma, mitä aluksi epäilin vaan konfiguraation suorittamisen erilaisuus. Molempien laitteiden IPSec VPN-yhteyden konfiguraatiosta oli saatavilla tietoa, mutta suurin osa näistä koski vain toisen laitevalmistajan laitteiden kesken tehtyjä konfiguraatioita.

Itselleni opinnäytetyön teko oli mieleinen ja erittäin haastava projekti. Työn edetessä opin erittäin paljon Juniper Networksin reitittimistä ja huomasin, kuinka suuri apu aikaisemmin tehdyistä opintojaksojen käytännön harjoitteista oikeasti oli. Ainut asia, joka työn tekemisessä jäi harmittamaan, oli työn pitkittyminen, mutta siitä ei voi ketään muuta syyttää kuin työn tekijää.

9.2 Tulokset ja tulevaisuus

Työssä saatiin testattua tavoitteiden mukaisesti tietoturvaminaisuudet, vaikka osaan niistä hieman ulkopuolista apua tarvittiinkin. Työn tuloksena saatiin toimiva testiympäristö, jossa tietoturvaominaisuuksien monipuolinen testaaminen ja niiden toimivuuden todentaminen on mahdollista. Tätä testiympäristöä ja konfiguraatioita käytetään työn liitteenä olevissa laboratorioharjoituksissa, joita on tarkoitus käyttää tulevilla tietoturvakursseilla käytännönharjoitteina.

Työn teoriaosuuden kokosin mielestäni mahdollisimman loogisessa järjestyksessä ja siten, että siitä olisi mahdollisimman paljon hyötyä tuleville tietoverkkotekniikan opiskelijoille ja mielestäni tässä myös onnistuin. Työn teoriaosuudesta tuli siis kattava peruspaketti Juniper Networks -reitittimien tietoturvaominaisuuksista, josta on varmasti hyötyä tuleville opiskelijoille.

Tulevaisuudessa mahdollisia jatkotutkimuksia voisi suorittaa IPSec VPN -yhteyksistä tai Intrusion Detection and Prevention -ominaisuuksista.

Lähteet

Bushong, M., Gadecki, C. & Garret, A. Junos for dummies.

Marschke, D. & Reynolds, H. JUNOS Enterprise Routing.

Juniper Networks Security Configuration Guide 2011. Versio 10.4. http://www.juniper.net/techpubs/en_US/junos10.4/information-products/topic-collections/security/software-all/security/index.html

Juniper Networks 2011a. Company Profile. Viitattu 15.4.2011. http://www.juniper.net/us/en/local/pdf/fact-sheets-backgrounder/3000054-en.pdf

Juniper Networks 2011b. JUNOS OS. The power of one operating system. Viitattu 15.4.2011. http://www.juniper.net/us/en/local/pdf/brochures/1500059-en.pdf

Jyväskylän Ammattikorkeakoulu 2011 a. Viitattu 15.4.2011. www.jamk.fi/tutustu

Jyväskylän Ammattikorkeakoulu 2011 b. Viitattu 15.4.2011. Tietotekniikan koulutus-ohjelma. http://www.jamk.fi/koulutus/tutkinnot/nuoret/tekniikanjaliikenteenala/tietotekniikka

Spidernet 2011. Viitattu 15.4.2011. http://student.labranet.jamk.fi/?page_id=121

Liitteet

Liite 1. Juniper-R5-konfiguraatiot

```
root@Juniper-R5# show
## Last changed: 2011-05-11 23:24:52 UTC
version 10.2R3.10;
system {
    root-authentication {
        encrypted-password "$1$MScTnDbq$OIhEQnQsrJz7Nk94aPnKt/"; ## SECRET-DATA
    }
    syslog {
        file testi {
            any any;
            security any;
        }
    }
}
interfaces {
    ge-1/0/2 {
        unit 0 {
            family inet {
                address 200.10.1.1/24;
            }
        }
    }
    ge-1/0/7 {
        vlan-tagging;
        unit 10 {
            vlan-id 10;
            family inet {
                address 192.168.1.1/25;
            }
        }
        unit 20 {
            vlan-id 20;
            family inet {
                address 192.168.1.129/25;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.4.1/32;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 172.16.1.2;
        route 192.168.3.0/24 next-hop st0.0;
    }
    router-id 172.168.2.1;
}
security {
    nat {
        source {
            pool pool1 {
                address {
                    200.10.1.129/32 to 200.10.1.142/32;
                }
            }
            rule-set rs-source {
                from zone wg1;
                to zone internet;
                rule r-source {
                    match {
                        source-address 192.168.1.129/25;
                        destination-address 0.0.0.0/0;
                    }
                    then {
                        source-nat {
```

```
                    pool {
                        pool1;
                    }
                }
            }
        }
    }
    static {
        rule-set rs-static {
            from zone internet;
            rule r-static {
                match {
                    destination-address 200.10.1.10/32;
                }
                then {
                    static-nat prefix 192.168.1.10/32;
                }
            }
        }
    }
    proxy-arp {
        interface ge-1/0/2.0 {
            address {
                200.10.1.10/32;
                200.10.1.129/32 to 200.10.1.142/32;
            }
        }
    }
}
screen {
    ids-option monitor {
        alarm-without-drop;
    }
    ids-option testi {
        icmp {
            large;
        }
    }
}
zones {
    security-zone internet {
        address-book {
            address wg3 192.168.3.128/25;
        }
        interfaces {
            ge-1/0/2.0 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                        all;
                    }
                }
            }
        }
    }
    security-zone server {
        address-book {
            address server 192.168.1.10/32;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-1/0/7.10;
        }
    }
    security-zone wg1 {
        address-book {
            address wg1 192.168.1.128/25;
```

```
            address admin 192.168.1.130/32;
            address wg3 192.168.3.128/25;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-1/0/7.20;
        }
    }
}
policies {
    from-zone server to-zone internet {
        policy 1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone internet to-zone server {
        policy 2 {
            match {
                source-address any;
                destination-address any;
                application junos-telnet;
            }
            then {
                deny;
            }
        }
        policy 1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
        policy kielto {
            match {
                source-address any;
                destination-address server;
                application any;
            }
            then {
                deny;
            }
        }
    }
    from-zone server to-zone wg1 {
        policy salli {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone wg1 to-zone server {
        policy admin {
            match {
                source-address admin;
```

```
                destination-address server;
                application any;
            }
            then {
                permit;
            }
        }
        policy deny_telnet {
            match {
                source-address any;
                destination-address any;
                application junos-telnet;
            }
            then {
                deny;
            }
        }
        policy basic_1 {
            match {
                source-address any;
                destination-address any;
                application [ junos-ftp junos-ssh ];
            }
            then {
                deny;
            }
        }
        policy basic_2 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone internet to-zone wg1 {
        policy 1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone wg1 to-zone internet {
        policy 1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
}
flow {
    tcp-mss {
        ipsec-vpn {
            mss 1350;
        }
    }
}
}
```

Liite 2. Juniper-R5-konfiguraatiot, reittipohjainen VPN-yhteys

root@Juniper-R5# show

```
## Last changed: 2011-05-12 21:47:15 UTC
version 10.2R3.10;
system {
    root-authentication {
        encrypted-password "$1$MScTnDbq$OIhEQnQsrJz7Nk94aPnKt/"; ## SECRET-DATA
    }
    syslog {
        file testi {
            any any;
            security any;
        }
    }
}
interfaces {
    ge-1/0/2 {
        unit 0 {
            family inet {
                address 200.10.1.1/24;
            }
        }
    }
    ge-1/0/7 {
        vlan-tagging;
        unit 10 {
            vlan-id 10;
            family inet {
                address 192.168.1.1/25;
            }
        }
        unit 20 {
            vlan-id 20;
            family inet {
                address 192.168.1.129/25;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.4.1/32;
            }
        }
    }
    st0 {
        unit 0 {
            family inet {
                address 10.10.10.10/24;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 200.10.1.2;
        route 192.168.3.128/25 next-hop st0.0;
        route 172.16.6.1/32 next-hop st0.0;
    }
    router-id 172.168.2.1;
}
security {
    ike {
        proposal ike-phase1-proposal {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm aes-128-cbc;
        }
        policy ike-phase1-policy {
            mode main;
            proposals ike-phase1-proposal;
            pre-shared-key ascii-text "$9$-uVYokqfz39GDnC"; ## SECRET-DATA
        }
        gateway gw-wg3 {
            ike-policy ike-phase1-policy;
            address 200.10.3.1;
            external-interface ge-1/0/2.0;
        }
```

```
}
ipsec {
    proposal ipsec-phase2-proposal {
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm aes-128-cbc;
    }
    policy ipsec-phase2-policy {
        perfect-forward-secrecy {
            keys group2;
        }
        proposals ipsec-phase2-proposal;
    }
    vpn ike-vpn-wg3 {
        bind-interface st0.0;
        vpn-monitor;
        ike {
            gateway gw-wg3;
            ipsec-policy ipsec-phase2-policy;
        }
        establish-tunnels immediately;
    }
}
nat {
    traceoptions {
        flag all;
    }
    source {
        pool pool1 {
            address {
                200.10.1.129/32 to 200.10.1.142/32;
            }
        }
        rule-set rs-source {
            from zone wg1;
            to zone internet;
            rule r-source {
                match {
                    source-address 192.168.1.128/25;
                    destination-address 0.0.0.0/0;
                }
                then {
                    source-nat {
                        pool {
                            pool1;
                        }
                    }
                }
            }
        }
    }
    static {
        rule-set rs-static {
            from zone internet;
            rule r-static {
                match {
                    destination-address 200.10.1.10/32;
                }
                then {
                    static-nat prefix 192.168.1.10/32;
                }
            }
        }
    }
    proxy-arp {
        interface ge-1/0/2.0 {
            address {
                200.10.1.10/32;
                200.10.1.129/32 to 200.10.1.142/32;
            }
        }
    }
}
screen {
    ids-option monitor {
        alarm-without-drop;
    }
```

```
    ids-option testi {
        icmp {
            large;
        }
    }
}
zones {
    security-zone internet {
        address-book {
            address wg3 192.168.3.128/25;
        }
        interfaces {
            ge-1/0/2.0 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                        all;
                    }
                }
            }
        }
    }
    security-zone server {
        address-book {
            address server 192.168.1.10/32;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-1/0/7.10;
        }
    }
    security-zone wg1 {
        address-book {
            address wg1 192.168.1.128/25;
            address admin 192.168.1.130/32;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-1/0/7.20;
        }
    }
    security-zone vpn-wg3 {
        address-book {
            address wg3 192.168.3.128/25;
        }
        interfaces {
            st0.0;
        }
    }
}
policies {
    from-zone internet to-zone wg1 {
        policy 1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
```

```
        }
      }
      from-zone wg1 to-zone internet {
        policy 1 {
          match {
            source-address any;
            destination-address any;
            application any;
          }
          then {
            permit;
          }
        }
      }
      from-zone wg1 to-zone vpn-wg3 {
        policy vpn-wg1-wg3 {
          match {
            source-address wg1;
            destination-address wg3;
            application any;
          }
          then {
            permit;
          }
        }
      }
      from-zone vpn-wg3 to-zone wg1 {
        policy vpn-wg3-wg1 {
          match {
            source-address wg3;
            destination-address wg1;
            application any;
          }
          then {
            permit;
          }
        }
      }
    }
    flow {
      tcp-mss {
        ipsec-vpn {
          mss 1350;
        }
      }
    }
}
```

Liite 3. Juniper-R5-konfiguraatiot, sääntöpohjainen VPN-yhteys

```
root@Juniper-R5# show
## Last changed: 2011-05-12 21:50:31 UTC
version 10.2R3.10;
system {
    root-authentication {
        encrypted-password "$1$MScTnDbq$OIhEQnQsrJz7Nk94aPnKt/"; ## SECRET-DATA
    }
    syslog {
        file testi {
            any any;
            security any;
        }
    }
}
interfaces {
    ge-1/0/2 {
        unit 0 {
            family inet {
                address 200.10.1.1/24;
            }
        }
    }
    ge-1/0/7 {
        vlan-tagging;
```

```
        unit 10 {
            vlan-id 10;
            family inet {
                address 192.168.1.1/25;
            }
        }
        unit 20 {
            vlan-id 20;
            family inet {
                address 192.168.1.129/25;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.4.1/32;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 200.10.1.2;
    }
    router-id 172.168.2.1;
}
security {
    ike {
        proposal ike-phase1-proposal {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm aes-128-cbc;
        }
        policy ike-phase1-policy {
            mode main;
            proposals ike-phase1-proposal;
            pre-shared-key ascii-text "$9$g2JZjTQnCpBGDnC"; ## SECRET-DATA
        }
        gateway gw-wg3 {
            ike-policy ike-phase1-policy;
            address 200.10.3.1;
            external-interface ge-1/0/2.0;
        }
    }
    ipsec {
        proposal ipsec-phase2-proposal {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-128-cbc;
        }
        policy ipsec-phase2-policy {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals ipsec-phase2-proposal;
        }
        vpn ike-vpn-wg3 {
            ike {
                gateway gw-wg3;
                ipsec-policy ipsec-phase2-policy;
            }
            establish-tunnels immediately;
        }
    }
    screen {
        ids-option monitor {
            alarm-without-drop;
        }
        ids-option testi {
            icmp {
                large;
            }
        }
    }
    zones {
```

```
    security-zone internet {
        address-book {
            address wg3 192.168.3.128/25;
        }
        interfaces {
            ge-1/0/2.0 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                        all;
                    }
                }
            }
        }
    }
    security-zone server {
        address-book {
            address server 192.168.1.10/32;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-1/0/7.10;
        }
    }
    security-zone wg1 {
        address-book {
            address wg1 192.168.1.128/25;
            address admin 192.168.1.130/32;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-1/0/7.20;
        }
    }
}
policies {
    from-zone internet to-zone wg1 {
        policy vpn-3-1 {
            match {
                source-address wg3;
                destination-address wg1;
                application any;
            }
            then {
                permit {
                    tunnel {
                        ipsec-vpn ike-vpn-wg3;
                        pair-policy vpn-1-3;
                    }
                }
            }
        }
    }
    from-zone wg1 to-zone internet {
        policy vpn-1-3 {
            match {
                source-address wg1;
                destination-address wg3;
                application any;
            }
            then {
```

```
                permit {
                    tunnel {
                        ipsec-vpn ike-vpn-wg3;
                        pair-policy vpn-3-1;
                    }
                }
            }
        }
        policy 1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    flow {
        tcp-mss {
            ipsec-vpn {
                mss 1350;
            }
        }
    }
}
```

Liite 4. Juniper-R5-konfiguraatiot, reittipohjainen VPN-yhteys Cisco Systemsin reitittimeen

```
root@Juniper-R5# show
## Last changed: 2011-05-12 21:53:30 UTC
version 10.2R3.10;
system {
    root-authentication {
        encrypted-password "$1$MScTnDbq$OIhEQnQsrJz7Nk94aPnKt/"; ## SECRET-DATA
    }
    syslog {
        file testi {
            any any;
            security any;
        }
    }
}
interfaces {
    ge-1/0/2 {
        unit 0 {
            family inet {
                address 200.10.1.1/24;
            }
        }
    }
    ge-1/0/7 {
        vlan-tagging;
        unit 10 {
            vlan-id 10;
            family inet {
                address 192.168.1.1/25;
            }
        }
        unit 20 {
            vlan-id 20;
            family inet {
                address 192.168.1.129/25;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.4.1/32;
            }
        }
    }
```

```
    st0 {
        unit 0 {
            family inet {
                address 172.16.1.1/32;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 200.10.1.2;
        route 172.16.5.1/32 next-hop st0.0;
        route 172.16.1.2/32 next-hop st0.0;
        route 192.168.2.128/25 next-hop st0.0;
    }
}
security {
    ike {
        proposal ike-phase1-proposal {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm aes-256-cbc;
            lifetime-seconds 300;
        }
        policy ike-phase1-policy {
            mode main;
            proposals ike-phase1-proposal;
            pre-shared-key ascii-text "$9$eAOW87g4ZjkPLxZj"; ## SECRET-DATA
        }
        gateway gw-cisco {
            ike-policy ike-phase1-policy;
            address 200.10.2.1;
            external-interface ge-1/0/2.0;
        }
    }
    ipsec {
        traceoptions {
            flag security-associations;
        }
        proposal ipsec-phase2-proposal {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-256-cbc;
            lifetime-seconds 300;
        }
        policy ipsec-phase2-policy {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals ipsec-phase2-proposal;
        }
        vpn ike-vpn-cisco {
            bind-interface st0.0;
            vpn-monitor;
            ike {
                gateway gw-cisco;
                ipsec-policy ipsec-phase2-policy;
            }
        }
    }
    screen {
        ids-option monitor {
            alarm-without-drop;
        }
        ids-option testi {
            icmp {
                large;
            }
        }
    }
    zones {
        security-zone internet {
            address-book {
                address wg3 192.168.3.128/25;
                address wg2 192.168.2.128/25;
            }
```

```
        interfaces {
            ge-1/0/2.0 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                        all;
                    }
                }
            }
        }
    }
    security-zone server {
        address-book {
            address server 192.168.1.10/32;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-1/0/7.10;
        }
    }
    security-zone wg1 {
        address-book {
            address wg1 192.168.1.128/25;
            address admin 192.168.1.130/32;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-1/0/7.20;
        }
    }
    security-zone vpn-cisco {
        address-book {
            address wg2 192.168.2.128/25;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            st0.0;
        }
    }
}
policies {
    default-policy {
        permit-all;
    }
}
traceoptions {
    file sec-debug;
    flag all;
}
flow {
    tcp-mss {
        ipsec-vpn {
            mss 1350;
        }
```

```
        }
    }
}

[edit]
root@Juniper-R5#
```

Liite 5. Juniper-R4-konfiguraatiot

```
root@Juniper-R4# show
## Last changed: 2011-05-12 21:55:08 UTC
version 10.2R3.10;
system {
    root-authentication {
        encrypted-password "$1$MScTnDbq$OIhEQnQsrJz7Nk94aPnKt/"; ## SECRET-DATA
    }
}
interfaces {
    ge-1/0/2 {
        unit 0 {
            family inet {
                address 200.10.3.1/24;
            }
        }
    }
    ge-1/0/7 {
        vlan-tagging;
        unit 50 {
            vlan-id 50;
            family inet {
                address 192.168.3.1/25;
            }
        }
        unit 60 {
            vlan-id 60;
            family inet {
                address 192.168.3.129/25;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.6.1/32;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 200.10.3.2;
    }
    router-id 172.168.6.1;
}
security {
        zones {
        security-zone internet {
            address-book {
                address wg1 192.168.1.128/25;
            }
            host-inbound-traffic {
                system-services {
                    ike;
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                ge-1/0/2.0;
            }
        }
        security-zone wg3 {
            address-book {
```

```
            address wg3 192.168.3.128/25;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-1/0/7.60;
        }
    }
    security-zone server {
        address-book {
            address server-wg3 192.168.3.10/32;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-1/0/7.50;
        }
    }
}
policies {
    from-zone wg3 to-zone server {
        policy 1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone server to-zone wg3 {
        policy 1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone internet to-zone wg3 {
        policy 1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone wg3 to-zone internet {
        policy 1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
```

```
            }
        }
    }
    from-zone server to-zone internet {
        policy 1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone internet to-zone server {
        policy 1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
}
flow {
    tcp-mss {
        ipsec-vpn {
            mss 1350;
        }
    }
}
}

[edit]
root@Juniper-R4#
```

Liite 6. Juniper-R4-konfiguraatiot, reittipohjainen VPN-yhteys

```
root@Juniper-R4# show
## Last changed: 2011-05-12 21:55:08 UTC
version 10.2R3.10;
system {
    root-authentication {
        encrypted-password "$1$MScTnDbq$OIhEQnQsrJz7Nk94aPnKt/"; ## SECRET-DATA
    }
}
interfaces {
    ge-1/0/2 {
        unit 0 {
            family inet {
                address 200.10.3.1/24;
            }
        }
    }
    ge-1/0/7 {
        vlan-tagging;
        unit 50 {
            vlan-id 50;
            family inet {
                address 192.168.3.1/25;
            }
        }
        unit 60 {
            vlan-id 60;
            family inet {
                address 192.168.3.129/25;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.6.1/32;
```

```
            }
        }
    }
    st0 {
        unit 0 {
            family inet {
                address 10.10.10.11/24;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 200.10.3.2;
        route 192.168.1.128/25 next-hop st0.0;
        route 172.16.2.1/32 next-hop st0.0;
    }
    router-id 172.168.6.1;
}
security {
    ike {
        proposal ike-phase1-proposal {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm aes-128-cbc;
        }
        policy ike-phase1-policy {
            mode main;
            proposals ike-phase1-proposal;
            pre-shared-key ascii-text "$9$VXwgJ.mT36ADi/t"; ## SECRET-DATA
        }
        gateway gw-wg1 {
            ike-policy ike-phase1-policy;
            address 200.10.1.1;
            external-interface ge-1/0/2.0;
        }
    }
    ipsec {
        proposal ipsec-phase2-proposal {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-128-cbc;
        }
        policy ipsec-phase2-policy {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals ipsec-phase2-proposal;
        }
        vpn ike-vpn-wg3 {
            bind-interface st0.0;
            vpn-monitor;
            ike {
                gateway gw-wg1;
                ipsec-policy ipsec-phase2-policy;
            }
            establish-tunnels immediately;
        }
    }
    zones {
        security-zone internet {
            address-book {
                address wg1 192.168.1.128/25;
            }
            host-inbound-traffic {
                system-services {
                    ike;
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                ge-1/0/2.0;
            }
```

```
    }
    security-zone wg3 {
      address-book {
        address wg3 192.168.3.128/25;
      }
      host-inbound-traffic {
        system-services {
          all;
        }
        protocols {
          all;
        }
      }
      interfaces {
        ge-1/0/7.60;
      }
    }
    security-zone vpn-wg3 {
      address-book {
        address wg1 192.168.1.128/25;
      }
      interfaces {
        st0.0;
      }
    }
    security-zone server {
      address-book {
        address server-wg3 192.168.3.10/32;
      }
      host-inbound-traffic {
        system-services {
          all;
        }
        protocols {
          all;
        }
      }
      interfaces {
        ge-1/0/7.50;
      }
    }
  }
  policies {
    from-zone wg3 to-zone vpn-wg3 {
      policy vpn-wg3-wg1 {
        match {
          source-address wg3;
          destination-address wg1;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone vpn-wg3 to-zone wg3 {
      policy vpn-wg1-wg3 {
        match {
          source-address wg1;
          destination-address wg3;
          application any;
        }
        then {
          permit;
        }
      }
    }
  }
  flow {
    tcp-mss {
      ipsec-vpn {
        mss 1350;
      }
    }
  }
}
```

```
[edit]
root@Juniper-R4#
```

Liite 7. Juniper-R4-konfiguraatiot, sääntöpohjainen VPN-yhteys

```
root@Juniper-R4# show
## Last changed: 2011-05-12 22:00:06 UTC
version 10.2R3.10;
system {
    root-authentication {
        encrypted-password "$1$MScTnDbq$OIhEQnQsrJz7Nk94aPnKt/"; ## SECRET-DATA
    }
}
interfaces {
    ge-1/0/2 {
        unit 0 {
            family inet {
                address 200.10.3.1/24;
            }
        }
    }
    ge-1/0/7 {
        vlan-tagging;
        unit 50 {
            vlan-id 50;
            family inet {
                address 192.168.3.1/25;
            }
        }
        unit 60 {
            vlan-id 60;
            family inet {
                address 192.168.3.129/25;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.6.1/32;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 200.10.3.2;
    }
    router-id 172.168.6.1;
}
security {
    ike {
        proposal ike-phase1-proposal {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm aes-128-cbc;
        }
        policy ike-phase1-policy {
            mode main;
            proposals ike-phase1-proposal;
            pre-shared-key ascii-text "$9$fzF/1IclvL36cl"; ## SECRET-DATA
        }
        gateway gw-wg3 {
            ike-policy ike-phase1-policy;
            address 200.10.1.1;
            external-interface ge-1/0/2.0;
        }
    }
    ipsec {
        proposal ipsec-phase2-proposal {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-128-cbc;
        }
```

```
    policy ipsec-phase2-policy {
        perfect-forward-secrecy {
            keys group2;
        }
        proposals ipsec-phase2-proposal;
    }
    vpn ike-vpn-wg3 {
        ike {
            gateway gw-wg3;
            ipsec-policy ipsec-phase2-policy;
        }
        establish-tunnels immediately;
    }
}
zones {
    security-zone internet {
        address-book {
            address wg1 192.168.1.128/25;
        }
        interfaces {
            ge-1/0/2.0 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                        all;
                    }
                }
            }
        }
    }
    security-zone wg3 {
        address-book {
            address wg3 192.168.3.128/25;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-1/0/7.60;
        }
    }
    security-zone server {
        address-book {
            address server-wg3 192.168.3.10/32;
        }
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-1/0/7.50;
        }
    }
}
policies {
    from-zone internet to-zone wg3 {
        policy vpn-1-3 {
            match {
                source-address wg1;
                destination-address wg3;
                application any;
            }
            then {
                permit {
                    tunnel {
                        ipsec-vpn ike-vpn-wg3;
```

```
                    pair-policy vpn-3-1;
                }
            }
        }
    }
    from-zone wg3 to-zone internet {
        policy vpn-3-1 {
            match {
                source-address wg3;
                destination-address wg1;
                application any;
            }
            then {
                permit {
                    tunnel {
                        ipsec-vpn ike-vpn-wg3;
                        pair-policy vpn-1-3;
                    }
                }
            }
        }
        policy 1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }

  }
  flow {
    tcp-mss {
      ipsec-vpn {
        mss 1350;
      }
    }
  }
}
```

Liite 8. WG2-R1-konfiguraatiot

```
wg2-r1#show runn
Building configuration...


Current configuration : 1960 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname wg2-r1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
!
dot11 syslog
no ip source-route
!
ip cef
!
no ip domain lookup
no ipv6 cef
vtp mode transparent
archive
```

```
 log config
  hidekeys
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
 lifetime 300
crypto isakmp key cisco address 200.10.1.1
!
crypto ipsec security-association lifetime seconds 300
!
crypto ipsec transform-set cisco esp-aes 256 esp-sha-hmac
!
crypto map cisco 10 ipsec-isakmp
 set peer 200.10.1.1
 set transform-set cisco
 set pfs group2
 match address 102
!
interface Loopback0
 ip address 172.16.5.1 255.255.255.255
!
interface GigabitEthernet0/0
 ip address 200.10.2.1 255.255.255.0
 duplex auto
 speed auto
 crypto map cisco
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.2.1 255.255.255.128
!
interface GigabitEthernet0/1.40
 encapsulation dot1Q 40
 ip address 192.168.2.129 255.255.255.128
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface FastEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 192.168.1.128 255.255.255.128 GigabitEthernet0/0
ip route 200.10.1.1 255.255.255.255 200.10.2.2
ip http server
no ip http secure-server
!
access-list 102 permit ip 192.168.2.128 0.0.0.127 192.168.1.128 0.0.0.127
!
control-plane
!
line con 0
line aux 0
```

```
line vty 0 4
 login
!
scheduler allocate 20000 1000
end

wg2-r1#
```

Liite 10. CiscoCore-R1-konfiguraatiot

```
Core-R1#show runn
Building configuration...

Current configuration : 1702 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Core-R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 25
!
!
ip cef
!
interface Loopback0
 ip address 130.0.3.1 255.255.255.252
!
interface ATM0/0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1/1
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 no ip address
 shutdown
 half-duplex
!
interface FastEthernet3/0
 no switchport
 ip address 130.0.0.10 255.255.255.252
!
interface FastEthernet3/1
 no switchport
 ip address 130.0.0.1 255.255.255.252
!
interface FastEthernet3/2
 no switchport
 ip address 200.10.1.2 255.255.255.0
!
interface FastEthernet3/3
!
```

```
interface FastEthernet3/4
!
interface FastEthernet3/5
!
interface FastEthernet3/6
!
interface FastEthernet3/7
!
interface FastEthernet3/8
!
interface FastEthernet3/9
!
interface FastEthernet3/10
!
interface FastEthernet3/11
!
interface FastEthernet3/12
!
interface FastEthernet3/13
!
interface FastEthernet3/14
!
interface FastEthernet3/15
!
interface GigabitEthernet3/0
!
interface Vlan1
 no ip address
!
router ospf 1
 log-adjacency-changes
 redistribute static metric-type 1
 network 130.0.0.0 0.0.0.3 area 0
 network 130.0.0.8 0.0.0.3 area 0
 network 130.0.3.0 0.0.0.3 area 0
 network 200.10.1.0 0.0.0.255 area 0
!
ip http server
no ip http secure-server
!
!
control-plane

!
line con 0
line aux 0
line vty 0 4
 login
!
!
end

Core-R1#
```

Liite 11. CiscoCore-R2-konfiguraatiot

```
Core-R2>ena
Core-R2#show runn
Building configuration...

Current configuration : 2086 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Core-R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 25
```

```
!
!
ip cef
!
interface Loopback0
 ip address 130.0.5.1 255.255.255.252
!
interface ATM0/0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
interface FastEthernet1/0
 description "Link to WG2-R1"
 ip address 200.10.2.2 255.255.255.0
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1/1
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 no ip address
 shutdown
 half-duplex
!
interface FastEthernet3/0
 description "Link to CiscoCore-R3"
 no switchport
 ip address 130.0.0.6 255.255.255.252
!
interface FastEthernet3/1
 description "Link to CiscoCore-R1"
 no switchport
 ip address 130.0.0.9 255.255.255.252
!
interface FastEthernet3/2
 shutdown
!
interface FastEthernet3/3
 shutdown
!
interface FastEthernet3/4
 shutdown
!
interface FastEthernet3/5
 shutdown
!
interface FastEthernet3/6
 shutdown
!
interface FastEthernet3/7
 shutdown
!
interface FastEthernet3/8
 shutdown
!
interface FastEthernet3/9
 shutdown
!
interface FastEthernet3/10
 no switchport
 ip address 130.0.10.1 255.255.255.252
!
interface FastEthernet3/11
 shutdown
!
interface FastEthernet3/12
 shutdown
!
```

```
interface FastEthernet3/13
 shutdown
!
interface FastEthernet3/14
 shutdown
!
interface FastEthernet3/15
 no switchport
 no ip address
 shutdown
!
interface GigabitEthernet3/0
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 redistribute static metric-type 1 subnets
 network 130.0.0.4 0.0.0.3 area 0
 network 130.0.0.8 0.0.0.3 area 0
 network 130.0.5.0 0.0.0.3 area 0
 network 130.0.10.0 0.0.0.3 area 0
 network 200.10.2.0 0.0.0.255 area 0
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
!
end
```

Liite 12. CiscoCore-R3-konfiguraatiot

```
Core-R3#show runn
Building configuration...

Current configuration : 1741 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Core-R3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 25
!
ip cef
!
interface Loopback0
 ip address 130.0.4.1 255.255.255.252
!
interface ATM0/0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
!
interface Serial1/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1/1
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet2/0
 no ip address
 shutdown
 half-duplex
!
interface FastEthernet3/0
 no switchport
 ip address 130.0.0.2 255.255.255.252
!
interface FastEthernet3/1
 no switchport
 ip address 130.0.0.5 255.255.255.252
!
interface FastEthernet3/2
 no switchport
 ip address 200.10.3.2 255.255.255.0
!
interface FastEthernet3/3
!
interface FastEthernet3/4
!
interface FastEthernet3/5
!
interface FastEthernet3/6
!
interface FastEthernet3/7
!
interface FastEthernet3/8
!
interface FastEthernet3/9
!
interface FastEthernet3/10
!
interface FastEthernet3/11
!
interface FastEthernet3/12
!
interface FastEthernet3/13
 no switchport
 no ip address
 shutdown
!
interface FastEthernet3/14
!
interface FastEthernet3/15
!
interface GigabitEthernet3/0
!
interface Vlan1
 no ip address
!
router ospf 1
 log-adjacency-changes
 redistribute static metric-type 1
 network 130.0.0.0 0.0.0.3 area 0
 network 130.0.0.4 0.0.0.3 area 0
 network 130.0.4.0 0.0.0.3 area 0
 network 200.10.3.0 0.0.0.255 area 0
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
```

```
line vty 0 4
 login
!
end

Core-R3#
```

Liite 13. WG1-SW1-konfiguraatiot

```
WG1-SW1#show runn
Building configuration...

Current configuration : 1760 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname WG1-SW1
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vtp domain wg1
vtp mode transparent
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan 10
 name Palvelin
!
vlan 20
 name Tyoasema
!
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/2
 description "Trunk to WG1-SW2"
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 speed 100
!
interface GigabitEthernet0/3
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/4
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/5
 description Virtual Debian
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/6
 description "Server"
 switchport access vlan 10
 switchport mode access
 speed 100
!
interface GigabitEthernet0/7
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/8
 description "Link to Centerswitch --> Juniper-R5"
```

```
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
interface GigabitEthernet0/9
 description Link to wg2-sw1
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/10
 description Link to wg5-sw1
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/11
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/12
 switchport mode dynamic desirable
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip http server
!
!
line con 0
line vty 0 4
 login
line vty 5 15
 login
!
end

WG1-SW1#
```

Liite 14. WG1-SW2-konfiguraatiot

```
wg1-sw2#show runn
Building configuration...

Current configuration : 2795 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg1-sw2
!
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vtp domain wg1
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
vlan 10
 name Palvelin
!
vlan 20
 name Tyoasema
!
interface FastEthernet0/1
 description Link to wg1-sw1
```

```
 switchport mode trunk
!
interface range FastEthernet0/2 - 12
 switchport access vlan 10
 switchport mode access
 shutdown
!
interface range FastEthernet0/13 - 24
 switchport access vlan 20
 switchport mode access
 shutdown
!
interface FastEthernet0/21
 description Virtual XP
 switchport access vlan 20
 switchport mode access
 speed 100
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan10
 ip address 192.168.1.2 255.255.255.128
 no ip route-cache
!
ip http server
!
line con 0
line vty 0 4
 login
line vty 5 15
 login
!
end

wg1-sw2#
```

Liite 15. WG2-SW1-konfiguraatiot

```
WG2-SW1#show runn
Building configuration...

Current configuration : 1740 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname WG2-SW1
!
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vtp domain wg3
vtp mode transparent
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan 30
 name Palvelin
!
vlan 40
 name Tyoasema
!
!
```

```
interface GigabitEthernet0/1
 description Link to wg2-r1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 30,40
 switchport mode trunk
!
interface GigabitEthernet0/2
 description "Trunk to WG2-SW2"
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 30,40
 switchport mode trunk
 speed 100
!
interface GigabitEthernet0/3
 description Link to wg3-sw3
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/4
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/5
 description Virtual Debian
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/6
 description "Server"
 switchport access vlan 50
 switchport mode access
 speed 100
!
interface GigabitEthernet0/7
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/8
 switchport mode dynamic desirable
!
interface GigabitEthernet0/9
 description Link to wg4-sw1
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/10
 description Link to wg2-sw1
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/11
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/12
 switchport mode dynamic desirable
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip http server
!
!
line con 0
line vty 0 4
 login
line vty 5 15
 login
!
!
end

WG2-SW1#
```

Liite 16. WG2-SW2-konfiguraatiot

```
wg2-sw2#show runn
Building configuration...

Current configuration : 2806 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg2-sw2
!
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vtp domain wg2
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
!
!
vlan 30
 name Palvelin
!
vlan 40
 name Tyoasema
!
interface FastEthernet0/1
 description Link to WG2-SW1
 switchport mode trunk
 speed 100
!
interface range FastEthernet0/2 - 12
 switchport access vlan 30
 switchport mode access
 shutdown
!
interface range FastEthernet0/13 - 24
 switchport access vlan 40
 switchport mode access
 shutdown
!
interface FastEthernet0/21
 description Virtual XP
 switchport access vlan 40
 switchport mode access
 speed 100
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan30
 ip address 192.168.2.2 255.255.255.128
 no ip route-cache
!
ip http server
!
line con 0
line vty 0 4
 login
line vty 5 15
 login
!
```

```
!
end

wg2-sw2#
```

Liite 17. WG3-SW1-konfiguraatiot

```
WG3-SW1#show runn
Building configuration...

Current configuration : 1827 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname WG3-SW1
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vtp domain wg3
vtp mode transparent
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan 50
 name Palvelin
!
vlan 60
 name Tyoasema
!
interface GigabitEthernet0/1
 description Link to wg3-r1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 shutdown
!
interface GigabitEthernet0/2
 description "Trunk to WG3-SW2"
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 50,60
 switchport mode trunk
 speed 100
!
interface GigabitEthernet0/3
 description Link to wg3-sw3
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/4
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/5
 description Virtual Debian
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/6
 description "Server"
 switchport access vlan 50
 switchport mode access
 speed 100
!
interface GigabitEthernet0/7
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/8
 description "Link to Centerswitch --> Juniper-R4"
```

```
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 50,60
 switchport mode trunk
!
interface GigabitEthernet0/9
 description Link to wg4-sw1
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/10
 description Link to wg2-sw1
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/11
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/12
 switchport mode dynamic desirable
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip http server
!
line con 0
line vty 0 4
 login
line vty 5 15
 login
!
end

WG3-SW1#
```

Liite 18. WG3-SW2-konfiguraatiot

```
wg3-sw2#show runn
Building configuration...

Current configuration : 2806 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg3-sw2
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vtp domain wg3
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
vlan 50
 name Palvelin
!
vlan 60
 name Tyoasema
!
interface FastEthernet0/1
 description Link to WG3-SW1
 switchport mode trunk
 speed 100
```

```
!
interface range FastEthernet0/2 - 12
 switchport access vlan 50
 switchport mode access
 shutdown
!
interface range FastEthernet0/13 - 24
 switchport access vlan 60
 switchport mode access
 shutdown
!
interface FastEthernet0/21
 description Virtual XP
 switchport access vlan 60
 switchport mode access
 speed 100
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan50
 ip address 192.168.3.2 255.255.255.128
 no ip route-cache
!
ip http server
!
line con 0
line vty 0
 login
line vty 5 15
 login
!
!
end

wg3-sw2#
```

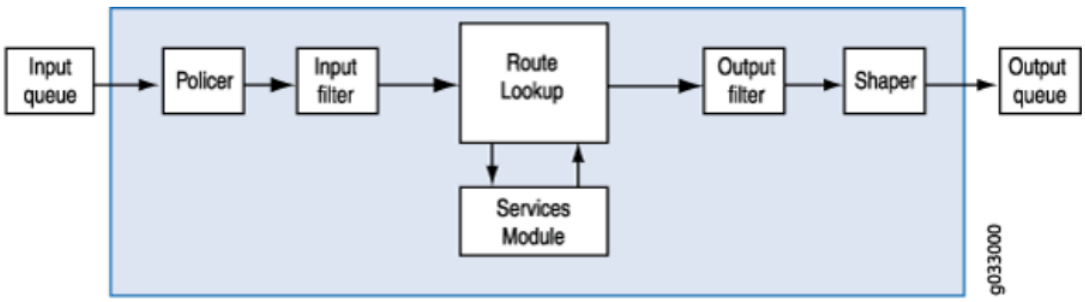
Jyväskylän ammattikorkeakoulu
Teknologia / ICT

Liite 19. Harjoitus: Security policyt, Screenit ja NAT

SISÄLTÖ

JOHDANTO

Paketit, jotka liikkuvat J-series-reitittimen sisälle tai ulos, käyvät läpi joko pakettipohjaisen (packet-based) prosessin tai vuopohjaisen (flow-based) prosessin. Pakettipohjaisella toimintaperiaatteella pakettien liikkuminen tapahtuu aina yksi paketti kerrallaan, eli jokaiselle paketille ominaisuuksista riippumatta käydään läpi aina sama prosessi (ks. kuvio 1).



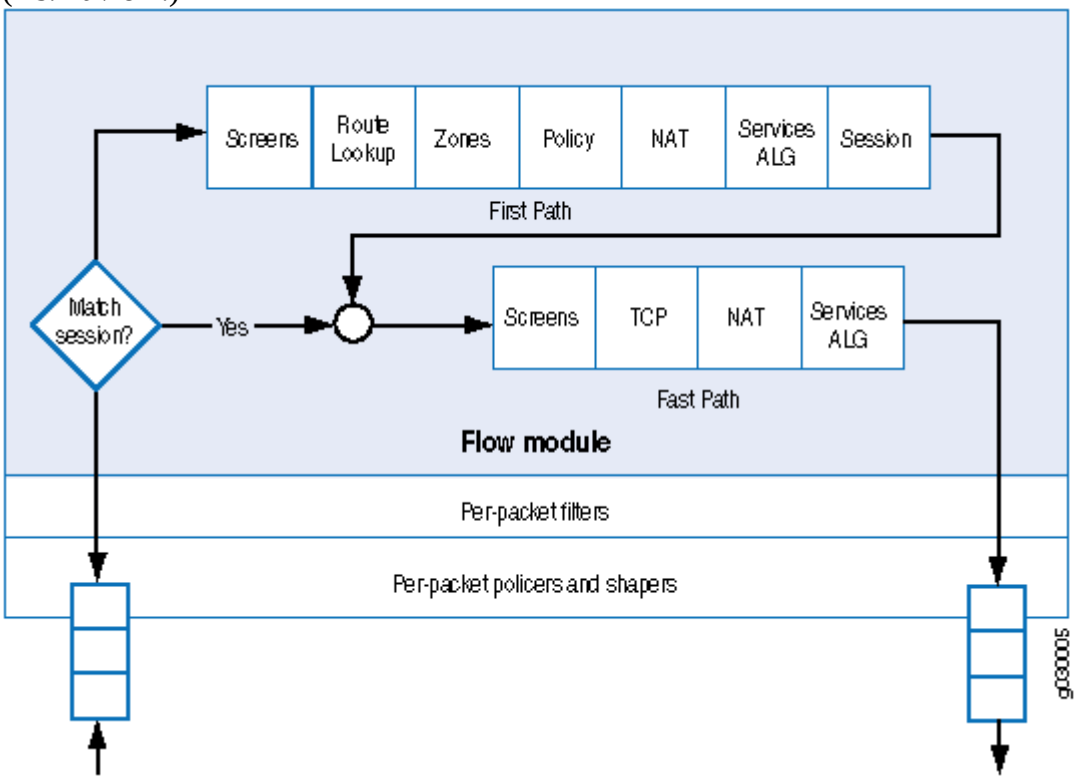
KUVIO 1. Pakettipohjainen prosessi

Vuopohjainen prosessi toimii aluksi samanlailla, kuin pakettipohjaisessakin, mutta seuraaville paketeille on luotu valmis istunto, joka nopeuttaa prosessointia. Paketeista tutkitaan seuraavat asiat:

1. Istunnon tunnus
2. Lähdeosoite
3. Kohdeosoite

4. Lähdeportti
5. Kohdeportti
6. Protokolla.

Jos nämä kriteerit täsmäävät, voidaan paketti laittaa samaan istuntoon, eli käytetään nopean polun prosessointia (Fast-Path Processing). Mikäli nämä kriteerit ei täyty, mennään jälleen pakettipohjaisen prosessoinnin mukaan (First-Packet Processing). (Ks. kuvio 2.)

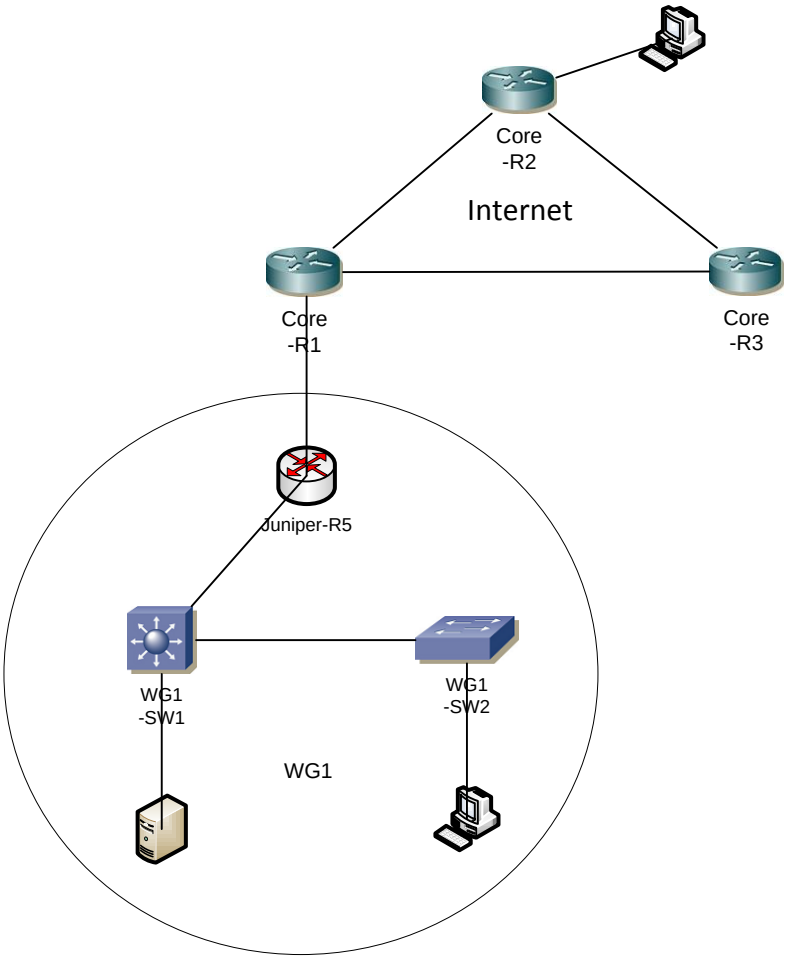


KUVIO 2. Vuopohjainen prosessi

Työnanto

Laboratorioharjoituksen tarkoituksena on päästä testaamaan Juniper J-series reitittimen tietoturvaominaisuuksia, kuten turvasäännöt (security policy), Screenit sekä Network Address Translation (NAT). Työssä konfiguroidaan kuvion 3 mukainen topologia.

Harjoitus: *Security policyt, Screenit ja NAT*



KUVIO 3. Laboratorioharjoituksen topologia

Internet

Työ aloitetaan konfiguroimalla ”Internet”, jota simuloidaan kolmella Cisco Core reitittimellä. Cisco Core –reitittimien välille konfiguroidaan OSPF-protokolla.

```
interface Loopback0
 ip address 130.0.3.1 255.255.255.252
!
interface FastEthernet3/0
 description "Link to CiscoCore-R2"
 no switchport
 ip address 130.0.0.10 255.255.255.252
!
interface FastEthernet3/1
```

```
 description "Link to CiscoCore-R3"
 no switchport
 ip address 130.0.0.1 255.255.255.252
!
interface FastEthernet3/2
 description "Link to Juniper-R5"
 no switchport
 ip address 200.10.1.2 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 network 130.0.0.0 0.0.0.3 area 0
 network 130.0.0.8 0.0.0.3 area 0
 network 130.0.3.0 0.0.0.3 area 0
 network 200.10.1.0 0.0.3 area 0
```

Konfiguraatiossa määritellään ensin tarvittavat IP-osoitteet rajapinnoille, jonka jälkeen konfiguroidaan OSPF ja mainostetaan tarvittavat verkot.

Työryhmä

Aloitetaan työryhmän konfigurointi kytkimestä WG1-SW2.

```
vlan 10
 name Palvelin
!
vlan 20
 name Tyoasema´
!
interface FastEthernet0/1
 description Link to wg1-sw1
 switchport mode trunk
!
interface FastEthernet0/21
 description Virtual XP
 switchport access vlan 10
 switchport mode access
 speed 100
```

Kytkimeen konfiguroidaan vain tarvittava rajapinta kytkimelle wg1-sw1 sekä virtuaalisen XP-koneen rajapinta.

Harjoitus: *Security policyt, Screenit ja NAT*

Seuraavaksi wg1-sw1:n konfigurointi:

```
interface GigabitEthernet0/2
 description "Trunk to WG1-SW2"
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10, 20
 switchport mode trunk
 speed 100
!
!
interface GigabitEthernet0/6
 description "Server"
 switchport access vlan 10
 switchport mode access
 speed 100
!
interface GigabitEthernet0/8
 description "Link to Centerswitch --> Juniper-R5"
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10, 20
 switchport mode trunk
```

Konfiguraatiossa muodostetaan ensin yhteys kytkimeen wg1-sw2, jonka jälkeen määritellään palvelimen rajapinta GigabitEthernet 0/6. Lopuksi konfiguroidaan linkkiväli WG1 →Juniper-R5.

Juniper-R5 konfigurointi:

```
}
interfaces {
    ge-1/0/2 {
        unit 0 {
            family inet {
                address 200.10.1.1/24;
            }
        }
    }
    ge-1/0/7 {
        vlan-tagging;
        unit 10 {
            vlan-id 10;
            family inet {
                address 192.168.1.1/25;
```

```
            }
        }
        unit 20 {
            vlan-id 20;
            family inet {
                address 192.168.1.129/25;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.4.1/32;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 172.16.1.2;
    }
    router-id 172.168.2.1;
}
```

Aluksi määritellään yhteys internetiin päin rajapintaan ge-1/0/2. Tämän jälkeen määritellään yhteys kyktimeen wg1-sw1 keskuskytkimen kautta. Lopuksi vielä Loopback rajapinta sekä staattinen reitti Internetiin päin.

Turva-alueet (Security Zone)

Seuraavilla konfiguraatioilla luodaan zone nimeltä wg1, jolle määritellään myös osoitekirja wg1.

```
root@Juniper-R5# set security zones security-zone wg1
root@Juniper-R5# edit security zones security-zone wg1
[edit security zones security-zone wg1]
root@Juniper-R5# set address-book address wg1 192.168.1.128/25
root@Juniper-R5# set host-inbound-traffic system-services all
root@Juniper-R5# set host-inbound-traffic protocols all
root@Juniper-R5# set interfaces ge-1/0/7.20
```

Luodaan samalla tavalla turva-alue *server:*

root@Juniper-R5# set security zones security-zone server
root@Juniper-R5# edit security zones security-zone server
[edit security zones security-zone server]
root@Juniper-R5# set address-book address wg1 192.168.1.0/25
root@Juniper-R5# set host-inbound-traffic system-services all
root@Juniper-R5# set host-inbound-traffic protocols all
root@Juniper-R5# set interfaces ge-1/0/7.10

Myös Internetille on luotava turva-alue. Alapuolella *show security zones* –komento, josta näkee mitä *Internet* turva-alueelle on määriteltävä.

```
security-zone internet {
    }
    interfaces {
        ge-1/0/2.0 {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
```

Turvasäännöt (Security Policy)

Turvasäännöt luodaan *from-zone to-zone* periaatteella. Seuraavan esimerkki säännöstä, joka koskee turva-alueelta *internet* tulevaa liikennettä turva-alueeseen *wg1*.

```
security {
        policies {
        from-zone internet to-zone wg1 {
            policy salli {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
```

Ja konfigurointi tapahtuu seuraavasti:

root@Juniper-R5# set security policies from-zone internet to-zone wg1 policy salli
root@Juniper-R5# edit security policies from-zone internet to-zone wg1 policy salli

Harjoitus: *Security policyt, Screenit ja NAT*

[edit security policies from-zone internet to-zone wg1 policy salli]
root@Juniper-R5# set match source-address any
root@Juniper-R5# set match destination address any
root@Juniper-R5# set match application any
root@Juniper-R5# set then permit

Luokaa samanlainen turvasääntö kuin yläpuolella, mutta toisin päin. Tässä säännössä siis kaikki liikenne sallitaan.

Tämän jälkeen luokaa sääntö, jolla kielletään telnet yhteys ”Internetin” Core-reitittimiin. Tässä esimerkki säännöstä, jolla tämä toteutetaan:

```
policies {
    from-zone wg1 to-zone internet {
        policy deny_telnet {
            match {
                source-address any;
                destination-address any;
                application junos-telnet;
            }
            then {
                deny;
            }
        }
```

Luokaa vielä säännöt, jossa kaikki liikenne sallitaan Internetistä palvelimelle ja myös toisin päin.

Screen

Screenit pitää sitoa turva-alueeseen, jotta ne aktivoituvat. Seuraavaksi esimerkki ICMP Large Screenin konfiguroinnista:

root@Juniper-R5# set security screen ids-option testi
root@Juniper-R5# edit security screen ids-option testi
[edit security screen ids-option testi]
root@Juniper-R5# set icmp large

Aluksi määritellään ids-option –kohtaan nimi, jolla Screeni ryhmä aktivoidaan turva-alueessa.

root@Juniper-R5#set security zones security-zone internet screen testi.
Aktiiviset Screenit voi tarkistaa menemällä Operational –tilaan, ja kirjoittamalla show security screen ids-option *testi*.

Harjoitus: *Security policyt, Screenit ja NAT*

```
root@Juniper-R5> show security screen ids-option testi
Screen object status:

Name                                                Value
  ICMP large packet                                 enabled

root@Juniper-R5>
```

KUVIO 4. Komento show security screen ids-option testi.

Generoikaa opettajan päättämällä ohjelmalla haittaliikennettä työryhmään ja yrittäkää tämän jälkeen estää hyökkäykset tai tiedusteluyritykset eri Screenejä käyttäen.

NAT

Työryhmässä on yksi palvelin sekä yksi virtuaalinen XP-kone. Asettakaa näille koneille IP-osoitteet. Käytän esimerkissä osoitteita:

Palvelin – 192.168.1.10/25
XP-kone – 192.168.1.130/25

Static NAT

Seuraavaksi muodostetaan staattinen NAT työryhmän palvelimelle:

set security nat static rule-set rs-static from zone internet
set security nat static rule-set rs-static rule r-static match destination-address 200.10.1.10/32
set security nat static rule-set rs-static rule r-static then static-nat prefix 192.168.1.10/32

Konfiguraatiossa määritellään aluksi sääntöryhmä (rule-set), johon liitetään tämän jälkeen säännöt (rule). Säännöksi konfiguraatiossa asetettiin turva-alueesta internet tulevien yhteyksien osoitteen muutoksen julkisesta osoitteesta 200.10.1.10/32, yksityiseen osoitteeseen 192.168.1.10/32.

set security nat proxy-arp interface ge-1/0/2.0 address 200.10.1.10/32

Lopuksi määritellään vielä rajapintaan ge-1/0/2.0 proxy-arp osoitteella 200.10.1.10/32, jotta rajapinta osaa käsitellä kyseisellä IP-osoitteella tulevat ARP -yhteys pyynnöt.

Source NAT

Seuraavaksi muodostetaan lähde NAT toimimaan yksityiselle aliverkolle 192.168.1.129/25.

set security nat source pool pool1 address 200.10.1.129/32 to 200.10.1.142/32
set security nat source rule-set rs-source from zone wg1
set security nat source rule-set rs-source to zone internet
set security nat source rule-set rs-source rule r-source match source-address 192.168.1.129/25
set security nat source rule-set rs-source rule r-source match destination-address 0.0.0.0/0
set security nat source rule-set rs-source rule r-source then source-nat pool pool1

Aluksi konfiguroidaan lähdeosoitteille osoiteryhmä (source address pool), johon myöhemmin konfiguraatiossa viitataan. Osoiteryhmään kuuluvat kaikki IP-osoitteet väliltä 200.10.1.129 – 200.10.1.142. Tämän jälkeen konfiguroidaan samalla tavalla, kuin staattisen NAT:n tapauksessakin, mutta nyt viitataan lopussa juuri luotuun osoiteryhmään.

set security nat proxy-arp interface ge-1/0/2.0 address 200.10.1.129/32 to 200.10.1.142/32

Lopuksi konfiguroidaan taas proxy-arp, rajapintaan ge-1/0/2.0 osoitteilla 200.10.1.129 - 200.10.1.142.

Tehtävät

1. Todistus security policyn toiminnasta, jolla kielletään telnet-yhteys.
2. Kuvankaappauksilla todistukset Screenien toimivuudesta. Testatkaa vähintään kolmea eri hyökkäys/tiedustelutapaa ja yrittäkää estää ne sen jälkeen.
3. Todistus staattisen NAT:n toimivuudesta.
4. Todistus source NAT:n toimivuudesta.

Jyväskylän ammattikorkeakoulu
Teknologia / ICT

Liite 20. Harjoitus: IPSEC VPN

SISÄLTÖ

JOHDANTO

Virtual Private Network (VPN)

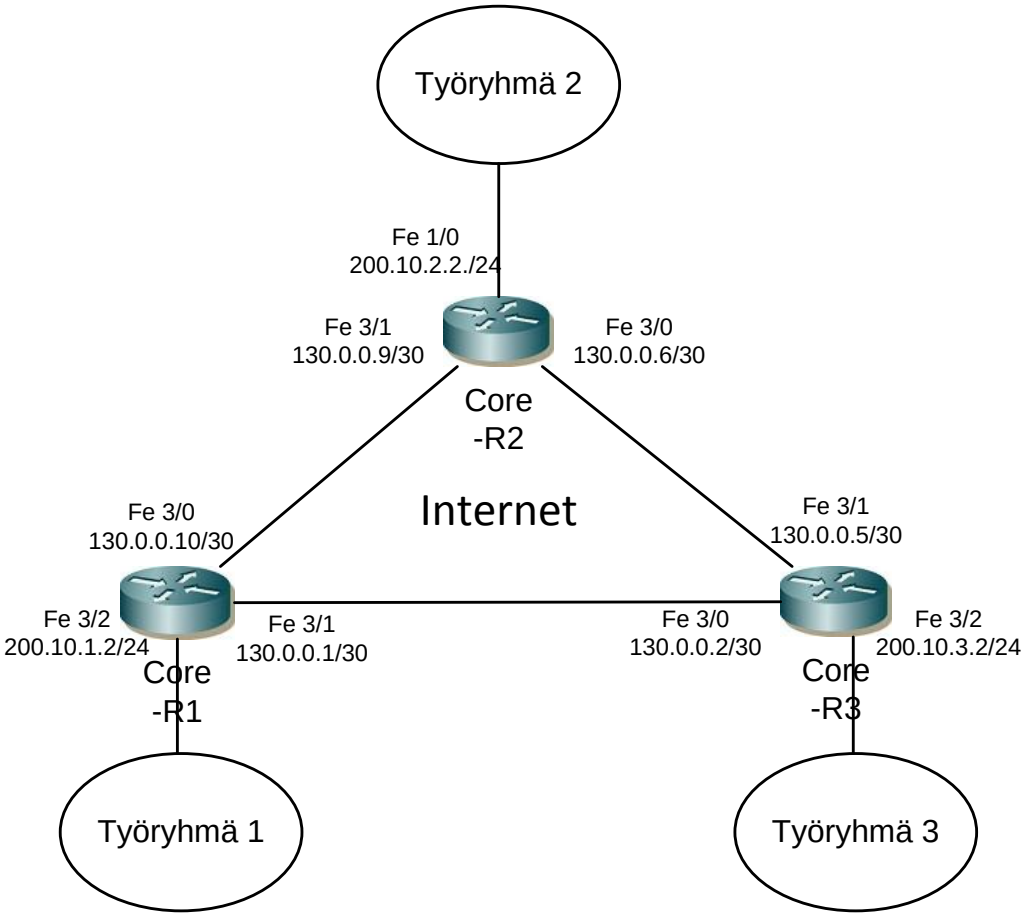
VPN-yhteys mahdollistaa kahden eri osapuolen turvallisen yhteyden Internetin yli. VPN-yhteys on mahdollista toteuttaa kahden verkon välille (site-to-site VPN) tai käyttäjän ja verkon välille. Liikenne näiden osapuolien välillä kulkee IP Security (IPsec) tunnelin välityksellä. IPsec on ryhmä TCP/IP protokollia, joilla turvataan liikenne Internetin yli. IPSec hoitaa liikenteen salauksen sekä osapuolten autentikoinnin.

Työnanto

Laboratorioharjoituksen tarkoituksena on muodostaa kaksi IPSec VPN -yhteyttä. Toinen yhteys muodostetaan Juniper Networksin reitittimien välille ja toinen Juniper Networksin sekä Cisco Systemsin -reitittimien välille.

Tehtävässä käytetään aikaisemmassa laboratorioharjoituksessa luotua ”Internetin” konfiguraatiota, sekä konfiguroidaan myös kaksi uutta työryhmää. Työryhmien yksi ja kolme konfiguraatiot ovat IP-osoitteita lukuunottamatta lähes identtiset. Työryhmässä kaksi korvataan Juniper Networksin reititin Cisco Systemsin laitteella. Harjoituksen työnannossa käydään ensin läpi esimerkkikonfiguraatiot kyseisistä VPN-yhteyksistä,

jonka jälkeen harjoituksen tekijä itse konfiguroi vastaavat konfiguraatiot. Harjoituksen topologia on kuviossa 1.



KUVIO 1. Topologia

Työryhmät yksi ja kolme

Työryhmän yksi konfiguraatio tehtiin jo aikaisemmassa laboratorioharjoituksessa (Harjoitus: Security Policyt, Screenit ja NAT). Työryhmän kolme konfigurointi tehdään samoilla komennoilla, kuin työryhmän yksi konfigurointi.

Työryhmän kaksi konfigurointi

Tässä työryhmässä laitteet wg2-sw1 ja wg2-sw2 konfiguroidaan samalla tavalla, kuin työryhmän yksi vastaavat laitteet, työryhmän omilla IP-osoitteilla.

Harjoitus: *IPSEC VPN*

Seuraavaksi tärkeimmät kohdat työryhmän kaksi reitittimen WG2-R1 konfiguroinnista:

```
interface GigabitEthernet0/0
 ip address 200.10.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 no shutdown
!
interface GigabitEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.2.1 255.255.255.128
!
interface GigabitEthernet0/1.40
 encapsulation dot1Q 40
 ip address 192.168.2.129 255.255.255.128

ip route 0.0.0.0 0.0.0.0 200.10.2.1
```

WG2-R1 konfiguroitiin ensin rajapinnoille tarvittavat IP-osoitteet, aktivoitiin dot1Q kapsulointi rajapinnoissa ge0/1.30 ja ge0/1.40. Lopuksi konfiguroitiin staattinen reitti CiscoCore-R2:lle.

Suorittakaa työryhmän kaksi ja kolme konfiguraatio sekä testatkaa yhteyksien toimivuus ja ottakaa tarvittavat kuvankaappaukset.

IPSec VPN (Juniper-Juniper)

IPSec VPN –yhteyden konfiguroiminen työryhmän yksi ja kolme välille tehdään sääntöpohjaisesti (policy based VPN). Alapuolella käytetään esimerkkinä Juniper-R5 laitteelle tehtyjä konfiguraatioita VPN-yhteyteen liittyen. Samat konfiguraatiot tehdään myös reitittimelle Juniper-R4, Juniper-R4-reitittimen näkökulmasta.

IKE avaintenvaihtoprosessin konfigurointi:

```
security {
    ike {
        proposal ike-phase1-proposal {
```

```
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
```

Aluksi konfiguroitiin ehdotus, jolle annettiin uniikki nimi, sekä määriteltiin autentikaatiomenetelmäksi *pre-shared-keys*, diffie-hellman ryhmäksi *group2*, autentikaatio-algoritmiksi *sha1* sekä tiedonsalaus-algoritmiksi *aes-128-cbc*.

```
policy ike-phase1-policy {
    mode main;
    proposals ike-phase1-proposal;
    pre-shared-key ascii-text "$9$-uVYokqfz39GDnC"; ## SECRET-DATA
```

Seuraavaksi konfiguroitiin sääntö *ike-phase1-policy*, joka sidottiin aikaisemmin tehtyyn ehdotukseen. Tässä määriteltiin myös yhteyden muodostamiseen käytettävä avain.

```
gateway gw-wg3 {
    ike-policy ike-phase1-policy;
    address 200.10.3.1;
    external-interface ge-1/0/2.0;
```

Lopuksi määriteltiin yhdyskäytävä *gw-wg3*, joka sidottiin sääntöön *ike-phase1-policy*. Yhdyskäytävälle määriteltiin laitteen ulospäin lähtevän liikenteen osoite 200.10.3.1 ja rajapinta ge-1/0/2.0.

Seuraavaksi konfiguroitiin IPSec:

```
ipsec {
    proposal ipsec-phase2-proposal {
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm aes-128-cbc;
```

Aluksi konfiguroitiin ehdotus, johon määriteltiin käytettäväksi protokolla *esp*, autentikointi algoritmi *hmac-sha1-96* sekä tiedonsalaus algoritmi *aes-128-cbc*.

```
policy ipsec-phase2-policy {
        perfect-forward-secrecy {
            keys group2;
        }
        proposals ipsec-phase2-proposal;
```

Harjoitus: *IPSEC VPN*

Seuraavaksi luotiin sääntö *ipsec-phase2-policy*, johon määriteltiin käytettäväksi *perfect-forwarf-secrecy* ja diffie hellman ryhmä *group2*. Tämän jälkeen sääntö sidottiin ehdotukseen.

```
vpn ike-vpn-wg3 {
    ike {
        gateway gw-wg3;
        ipsec-policy ipsec-phase2-policy;
    }
```

Lopuksi luotiin vpn:lle nimi *ike-vpn-wg3*, joka sidottiin aikaisemmin IKE-vaiheessa määriteltyyn yhdyskäytävään *gw-wg3* sekä policyyn *ipsec-phase2-policy*.

Kun IKE ja IPSec oli konfiguroitu, luotiin security policyt:

```
policies
    from-zone internet to-zone wg1 {
        policy vpn-3-1 {
            match {
                source-address wg3;
                destination-address wg1;
                application any;
            }
            then {
                permit {
                    tunnel {
                        ipsec-vpn ike-vpn-wg3;
                        pair-policy vpn-1-3;
                    }
    from-zone wg1 to-zone internet {
        policy vpn-1-3 {
            match {
                source-address wg1;
                destination-address wg3;
                application any;
            }
            then {
                permit {
                    tunnel {
                        ipsec-vpn ike-vpn-wg3;
                        pair-policy vpn-3-1;
```

Harjoitus: *IPSEC VPN*

Yläpuolella olevassa konfiguraatiossa määriteltiin lähde- ja kohdeosoitteet sekä määriteltiin liikenne menemään jo aikaisemmin luodun tunnelin *ike-vpn-wg3* kautta. Komennolla *pair-policy* sidottaan kaksi turvasääntöä, jotka käyttävät samaa VPN-tunnelia, käyttämään samaa SA:ta

Tehtävä 1

Toteuttakaa VPN-yhteyden konfiguroiminen työryhmien yksi ja kolme välille. Testatkaa yhteys pingaamalla sekä ottakaa kuvankaappaukset yhteyden todentamisesta. Hyödyllisiä komentoja:

show security ike security-associations
show security ipsec security-associations
show security ipsec statistics
show security flow session

IPSec VPN (Juniper-Cisco)

IPSec VPN –yhteyden konfiguroiminen työryhmän yksi ja kaksi välille tehdään reittipohjaisesti (route based VPN). Alapuolella on ensin esimerkki konfiguraatiosta Cisco Systemsin reitittimeltä WG2-R1, jonka jälkeen samat asetukset Juniper Networksin reitittimen Juniper-R5 konfiguraatioista.

Cisco

Ensin konfiguroidaan ISAKMP:

crypto isakmp policy 10
encr aes 256
authentication pre-share
group 2
lifetime 300
crypto isakmp key "avain" address 200.10.1.1

Aluksi määriteltiin ISAKMP sääntö *10*. Tiedonsalausalgoritmiksi määriteltiin AES 256kb, autentikointimenetelmäksi *pre-share*, Diffie-Hellman algoritmin ryhmä 2 sekä ISAKMP avaintenvaihdon elinikä komennolla *lifetime*. Lopuksi määriteltiin ISAKMP-yhteydelle avain, sekä kohdeosoite *200.10.1.1*, joka on Juniper-R5-reitittimen vastaanottava rajapinta Ge-1/0/2.

Harjoitus: *IPSEC VPN*

Seuraavaksi konfiguroidaan IPSec

crypto ipsec transform-set cisco esp-aes 256 esp-sha-hmac
crypto map cisco 10 ipsec-isakmp
set peer 200.10.1.1
set transform-set cisco
set pfs group2
match address 102

Konfigurointi aloitetaan määrittelemällä *transform-set*, johon määritellään. IPSEC-yhteydelle määritellään käytettäväksi protokollaksi *esp*, tiedonsalausalgoritmiksi *aes 256* sekä autentikointialgoritmiksi *sha-hmac*. Tämän jälkeen sidotaan IPSEC aikaisemmin luotuun ISAKMP sääntöön komennolla *crypto map cisco 10 ipsec-isakmp*. Edellisessä vaihesesa luotiin myös *crypto map* nimeltään cisco, johon liitetään *transform-set* cisco, määritellään yhteyden toisen osapuolen IP-osoite sekä asetetaan yhteys käyttämään Perfect Forward Secrecyä (PFS) Diffie-Hellman ryhmällä kaksi. Lopuksi määritellään vielä yhteys vertaamaan osoitteita Access Control List (ACL)-pääsylistaan 102. Pääsylistan konfigurointi alapuolella:

access-list 102 permit ip 192.168.2.128 0.0.0.127 192.168.1.128 0.0.0.127

Pääsylistassa 102 sallittiin yhteys reitittimeltä wg2-r1 reitittimeen Juniper-R5. Tämän jälkeen IPSec-yhteys sidottiin käytettävään rajapintaan GigabitEthernet0/0 sekä määriteltiin staattinen reititys.

interface GigabitEthernet0/0
ip address 200.10.2.1 255.255.255.0
crypto map cisco
!
ip route 192.168.1.128 255.255.255.128 GigabitEthernet0/0

Harjoitus: *IPSEC VPN*

Juniper

Ensin konfiguroidaan IKE

```
ike {
    proposal ike-phase1-proposal {
        authentication-method pre-shared-keys;
        dh-group group2;
        authentication-algorithm sha1;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 300;
    }
    policy ike-phase1-policy {
        mode main;
        proposals ike-phase1-proposal;
        pre-shared-key ascii-text "$9$eAOW87g4ZjkPLxZj"; ## SECRET-DATA
    }
    gateway gw-cisco {
        ike-policy ike-phase1-policy;
        address 200.10.2.1;
        external-interface ge-1/0/2.0;
    }
}
```

Junos-käyttöjärjestelmässä konfiguraatio aloitettiin tekemällä ehdotus (proposal), johon määriteltiin autentikointityyli, Diffie-Hellman ryhmä, autentikointialgoritmi, tiedonsalausalgoritmi sekä IKE ehdotukselle elinikä. Näihin konfiguraatioihin asetettiin samat arvot, kuin reitittimeen WG2-R1. Mikäli yksikin arvo näistä olisi konfiguroitu poikkeavasti toisesta osapuolesta, ei avaintenvaihtoprosessia pystyttäisi onnistuneesti suorittamaan. Lopuksi määriteltiin vielä oletusyhdyskäytävän nimi, IP-osoite sekä neuvotteluun käytettävä ulkoinen rajapinta.

Seuraavaksi konfiguroidaan IPSec

```
ipsec {
    }
    proposal ipsec-phase2-proposal {
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 300;
    }
```

```
policy ipsec-phase2-policy {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals ipsec-phase2-proposal;
}
vpn ike-vpn-cisco {
    bind-interface st0.0;
    ike {
        gateway gw-cisco;
        ipsec-policy ipsec-phase2-policy;
    }
}
```

Yläpuolella olevassa konfiguraatiossa määriteltiin ensin ehdotus *ipsec-phase2-proposal*. Tämän jälkeen määriteltiin IPSec sääntö *ipsec-phase2*-policy, joka liitettiin ehdotukseen. Ehdotukseen ja sääntöön asetettiin samat asetukset, kuin WG2-R1 reitittimeenkin. Lopuksi luotiin VPN nimeltä *ike-vpn-cisco*, johon liitettiin rajapinnaksi *st0.0*, IKE yhdyskäytäväksi aikaisemmin luotu *gw-cisco* sekä sääntö *ipsec-phase2-policy*.

Juniper-R5 reitittimeen asetettiin rajapinta *st0.0* sekä staattinen reitti kulkemaan tämän rajapinnan kautta reitittimeen WG2-R1.

```
st0 {
    unit 0 {
        family inet {
            address 172.16.1.1/32;
        }
    }
}
routing-options {
    static {
        route 192.168.2.128/25 next-hop st0.0;
    }
}
```

Harjoitus: *IPSEC VPN*

Tehtävä 2

Toteuttakaa VPN-yhteyden konfiguroiminen työryhmien yksi ja kaksi välille. Testatkaa yhteys pingaamalla sekä ottakaa kuvankaappaukset yhteyden todentamisesta. Hyödyllisiä komentoja:

Junos
show security ike security-associations
show security ipsec security-associations
show security ipsec statistics
show security flow session

Cisco
show crypto isakmp policy
show crypto isakmp sa
show crypto ipsecc sa
show crypto session